

Dohoda o integračnom zámere spoločnosti DÔVERA zdravotná poisťovňa a. s. a Národného centra zdravotníckych informácií pre sprístupňovanie digitálneho COVID preukazu EÚ (ďalej aj len „Dohoda“)

Subjekt	Národné centrum zdravotníckych informácií Sídlo: Lazaretská 26 811 09 Bratislava IČO: 00165387	Subjekt	DÔVERA zdravotná poisťovňa a. s. Sídlo: Einsteinova 25, 851 01 Bratislava IČO: 35 942 436
Meno	Ing. Pavol Capek	Meno	Martin Fojtik
Funkcia	generálny riaditeľ	Funkcia	riaditeľ úseku IT
Dátum		Dátum	
Podpis		Podpis	

Projekt:	Integrácia aplikácie Smart Cert App na DÔVERA zdravotná poisťovňa a.s.
Dokument:	DIZ-Dovera-SCA_1.0.docx
Verzia:	1.0
Dátum:	29.6.2021
Autor:	
Vlastník:	Národné centrum zdravotníckych informácií

História dokumentu

Verzia	Dátum verzie	Popis zmien	Vypracoval
0.1	7.6.2021	Iniciálny dokument	
0.2	18. 6. 2021	Doplnenie za Dôvera zdravotná poisťovňa, a.s.	
0.3	23.6.2021	Doplnenie za NCZI, otvorené otázky	
0.4	24.6.2021	Doplnenie za Dôvera zdravotná poisťovňa, a.s.	
0.5	28.6.2021	Doplnenie za NCZI	
0.6	29.6.2021	Doplnenie za Dôvera zdravotná poisťovňa, a.s.	
1.0	29.6.2021	Doplnenie za NCZI	

Obsah

SKRATKY A POJMY	4
1 ÚVODNÉ USTANOVENIA	5
1.1 IDENTIFIKÁCIA SUBJEKTOV INTEGRAČNÉHO ZÁMERU.....	5
1.2 ZDÔVODNENIE A CIELE INTEGRAČNÉHO ZÁMERU	5
1.3 ROZPOČET	5
2 ROZSAH INTEGRÁCIE	6
2.1 ARCHITEKTÚRA RIEŠENIA SCA	6
2.2 POPIS HLAVNÝCH SLUŽIEB VYUŽÍVANÝCH V PROCESOCH	7
2.3 POPIS PROCESOV SÚVISIACICH S POSKYTNUTÍM ÚDAJOV ZO SCA PRE IS DZP.....	7
2.3.1 Zobrazenie informácií v mobilnej aplikácii	7
2.3.2 Vytlačenie certifikátu klientovi na pobočke	7
2.4 ARCHITEKTÚRA RIEŠENIA IS DZP	7
2.5 KOMUNIKÁCIA MEDZI IS DZP A SCA	8
2.5.1 Procesy IS DZP z pohľadu komunikácie voči SCA	9
2.5.2 Frekvencia a objem komunikácie voči SCA	9
2.6 AUDITNÉ LOGOVANIE	9
2.7 TESTOVACIE SCENÁRE	9
2.8 AUTENTIFIKÁCIA KONEČNÝCH UŽÍVATEĽOV.....	10
2.9 PRÍSTUP NA PROSTREDIA - CERTIFIKÁTY A KLÚČE	10
3 KOMUNIKAČNÝ PLÁN	10
3.1 POPIS ROLÍ A ZODPOVEDNOSTI	10
3.2 KOMUNIKAČNÉ PROCESY	11
4 HARMONOGRAM	12
4.1 POPIS HARMONOGRAMU	12
4.2 NEVYHNUTNÉ PODMIENKY	13
4.3 EXTERNÉ ZÁVISLOSTI	13
5 MLČANLIVOSŤ A OCHRANA DÔVERNÝCH INFORMÁCIÍ	14
6 SPRACÚVANIE OSOBNÝCH ÚDAJOV A ZÁRUKY ZA OCHRANU OSOBNÝCH ÚDAJOV 14	
7 ZÁVEREČNÉ USTANOVENIA	16

Skratky a pojmy

NCZI	Národné centrum zdravotníckych informácií
DIZ alebo Dohoda	táto Dohoda o integračnom zámere
SCA	Informačný systém Smart Cert App
IS	Informačný systém
API	Application programming interface alebo skratkou API (rozhranie pre programovanie aplikácií)
CA	Certifikačná autorita
COVID preukaz EÚ alebo certifikát	potvrdenia obsahujúce informácie o držiteľovom očkovaní, výsledku testu alebo prekonaní ochorenia vydané v súvislosti s pandémiou ochorenia COVID-19
IP	Internetový protokol
Nariadenie o DCC	nariadenie Európskeho parlamentu a Rady (EÚ) 2021/953 zo 14. júna 2021 o rámci pre vydávanie, overovanie a uznávanie interoperabilných potvrdení o očkovaní proti ochoreniu COVID-19, o vykonaní testu a prekonaní tohto ochorenia (digitálny COVID preukaz EÚ) s cieľom uľahčiť voľný pohyb počas pandémie ochorenia COVID-19
mTLS	Mutual authentication
DZP	DÔVERA zdravotná poisťovňa a. s.
ESB	Enterprise Service Bus

1 Úvodné ustanovenia

1.1 Identifikácia subjektov integračného zámeru

Subjektmi Dohody o integračnom zámere sú Národné centrum zdravotníckych informácií (NCZI) a DÔVERA zdravotná poisťovňa a. s. (ďalej ako „DZP“). Konzumentom riešenia v rámci integrácie bude Mobilná aplikácia DZP, poskytovateľom riešenia bude IS Smart Cert App

Subjekty Dohody	Rola	Správca (Gestor)	IS spadajúce pod Dohodu
	Konzument	DÔVERA zdravotná poisťovňa a. s. Einsteinová 25 851 05 35942436	Mobilná aplikácia
	Poskytovateľ	Národné centrum zdravotníckych informácií, so sídlom: Lazaretská 26, 811 09 Bratislava IČO: 00165387	Smart Cert App

1.2 Zdôvodnenie a ciele integračného zámeru

NCZI a DZP uzatvárajú túto Dohodu za účelom realizácie sprístupňovania digitálneho COVID preukazu EÚ alebo COVID preukazu EÚ v listinnej podobe poistencom DZP.

Integrácia vyplýva z navrhovanej legislatívy SR a požiadaviek EÚ na harmonizáciu procesov pre vydávanie a preukazovanie sa certifikátmi o vakcinácii osoby, výsledkoch testu na COVID-19 a potvrdení o prekonaní ochorenia COVID-19. Návrh a implementácia riešenia umožní poistencom využívať štandardné riešenie digitálnej a papierovej verzie certifikátu a pomôže automatizovať procesy v súlade s usmerneniami EÚ a internými metodikami SR.

Subjekty tejto Dohody sa zaväzujú bezodplatne navzájom spolupracovať a poskytovať si všetku potrebnú súčinnosť na dosiahnutie účelu tejto Dohody, v súlade s ustanoveniami tejto Dohody a príslušnými právnymi predpismi.

1.3 Rozpočet

Náklady na integráciu informačných systémov SCA a DZP sú hradené na každej strane zvlášť zo samostatných rozpočtových položiek projektov oboch subjektov Dohody.

2 Rozsah integrácie

Sekcia zachytáva rozsah integrácie z pohľadu komplexnosti integrovaných biznis procesov a požiadaviek na funkcionality/služby.

Názov API rozhrania Smart Cert App
Smart Cert App verified read

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

2.1 Architektúra riešenia SCA

Nižšie je zobrazená aplikačná architektúra SCA, vrátane zakreslených aktuálne plánovaných komunikačných kanálov.

2.2 Popis hlavných služieb využívaných v procesoch

API Smart Cert App verified read je realizované ako samostatný host na jednej public IP s definovanými mTLS pravidlami nezávisle od iných hostov na rovnakom API (samostatná CA, samostatný server cert pre daný host, samostatné klientske prístupy).

Ako dodatočná ochrana je designovaný IP whitelisting na úrovni cloud providera pre verejnú IP.

Prostredia: DEV, TEST, PREPROD, PROD

Samotný popis rozhrania je cez "Swagger" dokumentáciu, zaslanú separátne mimo DIZ.

2.3 Popis procesov súvisiacich s poskytnutím údajov zo SCA pre IS DZP

2.3.1 Zobrazenie informácií v mobilnej aplikácii

Poistenec DZP sa prihlási do mobilnej aplikácie svojimi prihlasovacími údajmi. Po overení identity si v menu vyberie položku pre zobrazenie certifikátu. Na pozadí sa zavolá interná služba ESB DZP publikovaná v DMZ. Služba zavolá SCA na dodanom endpointe. Postupne volá metódy v poradí:

1. /sub/check – overenie rodného čísla
2. /dgc/{subid} – zoznam certifikátov
3. /dgc/{subid}/{dgcid}/pdf - PDF súbor s certifikátom
 - a. alt. /dgc/{subid}/{dgcid}/data – štruktúrované data
 - b. alt. /dgc/{subid}/{dgcid}/qrc – obrázok s QR kódom

2.3.2 Vytlačenie certifikátu klientovi na pobočke

Poistenec DZP príde na pobočku zdravotnej poisťovne. Zamestnanec DZP overí jeho totožnosť. Zamestnanec DZP si v IS DZP zobrazí kartu poistenca a na jeho žiadosť požiadá o prevzatie PDF výstupu z SCA. Na pozadí sa zavolá interná služba ESB DZP publikovaná v DMZ. Služba zavolá SCA na dodanom endpointe. Postupne volá metódy v poradí:

1. /sub/check – overenie rodného čísla
2. /dgc/{subid} – zoznam certifikátov
3. /dgc/{subid}/{dgcid}/pdf - PDF súbor s certifikátom

Pre tento scenár nebudú využívané alternatívy vo forme štruktúrovaných dát a obrázku QRC.

2.4 Architektúra riešenia IS DZP

Návrh spočíva v zriadení novej internej služby na ESB DZP publikovaná v DMZ.

Služba bude zabezpečovať komunikáciu DZP vs. SCA ako Single-Point-Of-Contact pre účely tejto implementácie. Teda:

1. Prevezme požiadavku zo zdrojového systému (MOA server, resp. CRM systém)
2. Vykoná volania voči SCA (podľa 2.3.1, resp. 2.3.2)
3. Spracuje odpoveď z SCA
4. Vráti spracovanú odpoveď do zdrojového systému IS DZP (MOA server, resp. CRM systém)
5. Zapíše auditný log na ESB + informáciu o výsledku (OK/NOK a chybu spracovania).

2.5 Komunikácia medzi IS DZP a SCA

Postup komunikácie z MOA:

1. Poistenec si vo svojej mobilnej aplikácii vyberie položku na zobrazenie očkovacieho certifikátu.
2. Mobilná aplikácia vytvorí spojenie s MOA serverom, ktorý zastrešuje všetku komunikáciu medzi jednotlivými aplikáciami a IS DZP
3. MOA server zavolá internú ESB, na ktorej je publikovaná kompozitná služba pre volanie SCA.
4. Interná ESB vykoná volania voči SCA (overenie rodného čísla, zoznam certifikátu, detail certifikátu vo forme PDF, príp. v štruktúrovanej forme a QRC kód.
5. Interná ESB vráti výstup vo formáte PDF na MOA server.
6. MOA server vráti výstup do príslušnej klientskej aplikácie.
7. Mobilná aplikácia zobrazí výstup na obrazovke.
8. Celá komunikácia je synchrónna.

Postup komunikácie z klientskej pobočky:

1. Zamestnanec DZP overí totožnosť poistenca v súlade s internými procesmi DZP.
2. Zamestnanec DZP v CRM systéme zobrazí kartu poistenca, ktorý sa nachádza na pobočke. Na žiadosť poistenca klikne na tlačidlo pre stiahnutie PDF s certifikátom.
3. CRM aplikácia zavolá internú ESB, na ktorej je publikovaná kompozitná služba pre volanie SCA.
4. Interná ESB vykoná volania voči SCA (overenie rodného čísla, zoznam certifikátu, detail certifikátu vo forme PDF, príp. v štruktúrovanej forme a QRC kód.
5. Interná ESB vráti výstup vo formáte do klientskej aplikácie CRM príslušného zamestnanca DZP.
6. Zamestnanec DZP vytlačí očkovací certifikát klientovi a odovzdá ho poistencovi.
7. Celá komunikácia je synchrónna.

2.5.1 Procesy IS DZP z pohľadu komunikácie voči SCA

2.5.2 Frekvencia a objem komunikácie voči SCA

Služba bude na internej ESB DZP dostupná 24x7. Rovnako komunikácia z mobilných aplikácií je dostupná 24x7. Komunikácia z pobočiek je potrebná v pracovných hodinách spravidla 8x5.

V mobilnej aplikácii sa denne pohybuje cca 25 tisíc ľudí. Predpoklad je, že cca 30% klientov si požiada o zobrazenie očkovacieho certifikátu. V peakoch môže byť počet volaní 50 - 80 za minútu.

DZP nastaví komunikáciu tak, aby frekvencia neprekročila 500 paralelných spojení, ktoré budú SCA vybavené do 500 ms.

2.6 Auditné logovanie

Popis logovania (aplikačného, bezpečnostného a prevádzkového) v IS DZP

V prostredí internej CRM aplikácie ide o existujúci log:

- identifikácia zamestnanca DZP, ktorý pristupuje na záznamy poistenca
- identifikácia poistenca DZP
- časovú pečiatku volania

V prostredí ESB ide o prevádzkový log konkrétneho volania:

- Zdrojový systém (MOA, CRM)
- Request volania
- Response volania – v tomto prípade bez osobných údajov, vid' nižšie
- Dátum a čas volania a jeho trvanie

Doba uchovávanía logov musí byť minimálne 6 mesiacov.

IS DZP nebude ukladať samotné výstupy metód SCA (obsahy dokumentov, štruktúrované dáta, obrázky).

2.7 Testovacie scenáre

Testovacie scenáre budú zrealizované podľa dostupných dát-certifikátov v testovacom prostredí tak, aby boli preverené jednotlivé typy certifikátov a aj rôzne počty a typy certifikátov v rámci zoznamu certifikátov pre jedného užívateľa. Testovacie scenáre tvoria Prílohu č. 1 tejto Dohody.

2.8 Autentifikácia konečných užívateľov

Poistenci sú overovaní prostredníctvom existujúcich procesov DZP tak aby bola zabezpečená jednoznačná identifikácia poistenca. Do mobilnej aplikácie majú pridelené prihlasovacie údaje. Na pobočke sú overení manuálne v súlade s internými procesmi DZP.

2.9 Prístup na prostredia - certifikáty a kľúče

Pre komunikáciu na zabezpečených API je potrebné využívať bezpečnostné certifikáty a kľúče, ktoré NCZI dodá DZP vopred dohodnutým a zabezpečeným spôsobom, ktorý bude dohodnutý samostatne pre každé jedno prostredie. Pre každé prostredie bude určený mechanizmus distribúcie a prevzatia certifikátov a kľúčov. Po prevzatí certifikátov a kľúčov bude za ich zabezpečenie pred kompromitáciou a únikom z prostredia DZP zodpovedať DZP.

Pre prístup cez zabezpečené API musí Konzument zabezpečiť overenie osoby, ktorej spracované údaje sú získane od Poskytovateľa, vlastnými mechanizmami, aby bola dodržaná dôvernosť údajov. Akceptovaným mechanizmom v rámci dotazovanej aplikácie Konzumenta je overenie osoby napríklad pomocou RFO alebo iným relevantným spôsobom.

Poskytovateľ zabezpečuje ochranu údajov v súlade s DIZ na úrovni API. Konzument zodpovedá za bezpečnosť spracovávaných údajov poskytnutých poskytovateľom, ktoré sú prenášané a spracovávané mimo API rozhranie. Súčasne konzument zodpovedá za bezpečnosť požiadaviek (requestov), ktoré sú na API Poskytovateľa zasielané z IS DZP.

Zodpovednosť za bezpečnosť údajov spracovávaných jednotlivými stranami (Poskytovateľom a Konzumentom) je definovaná rozhraním poskytovaného API SCA. Zodpovednosť za bezpečnosť a ochranu poskytnutých údajov na úrovni API SCA zabezpečuje Poskytovateľ. Údaje mimo informačný systém SCA, ktoré boli poskytnuté formou API SCA pre aplikáciu GreenPass ako aj do systému IS GreenPass sú v zodpovednosti Konzumenta.

V prípade identifikácie bezpečnostného incidentu súvisiaceho s kybernetickou bezpečnosťou je potrebné eskalovať informácie manažérovi kybernetickej bezpečnosti NCZI. V súvislosti s incidentami ohľadom narušenia bezpečnosti osobných údajov je potrebné kontaktovať DPO oboch strán.

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 spoločnosť DZP	Poskytovateľ SCA
Projektový manažér		
Hlavný biznis analytik		
Hlavný architekt alebo technický návrhár		
Integračný manažér		
Test manažér		

Rola	Konzument spoločnosť DZP	Poskytovateľ SCA
Prevádzka a infraštruktúra		
Bezpečnostný architekt		
Incident manažér		

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 manažérmi
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
Bezpečnosť	Definovanie požiadaviek, analýza, testy	Bezpečnostne požiadavky na výmenu informácií, na prístup a aplikáciu, bezpečnostné testovania, riziká,
Eskalácia na PM	1. stupeň	Zápis

4 Harmonogram

4.1 Popis harmonogramu

Aktivita	Vstup	Výstup	Dátum začiatku	Dátum Ukončenia	Závislosti aktivít	Zodpovedná osoba
Vypracovanie integračnej dokumentácie	Integračný manuál, Integračný zámer	Informácie v katalógu služieb, Integračný manuál poskytovanej služby, Model využívaných služieb, Návrh variantov pre naplnenie požiadaviek, Integračný technický návrh, Testovací plán, Protokol o pripravenosti technického návrhu integrácie	18.6.2021	29.6.2021		Projektový manažér, Hlavný architekt alebo technický návrhár
Prepojenie testovacej infraštruktúry	Výstup predchádzajúcich aktivít	Špecifikácia prepojenia testovacej infraštruktúry, Protokol o pripravenosti testovacej infraštruktúry	18.6.2021	21.6.2021	Vypracovanie integračnej dokumentácie	Projektový manažér, Prevádzka a infraštruktúra
Príprava a vykonanie integračných testov	Výstupy predchádzajúcich aktivít Testovacie dáta	Testovacie scenáre a testovacie prípady integračného testovania, Protokol o ukončení integračných testov, Aktualizovaná relevantná dokumentácia integrácie (v prípade potreby)	21.6.2021	25.6.2021	Prepojenie testovacej infraštruktúry	Projektový manažér, Test manažér

Aktivita	Vstup	Výstup	Dátum začiatku	Dátum Ukončenia	Závislosti aktivít	Zodpovedná osoba
Príprava a vykonanie používateľských akceptačných testov (UAT)	Výstupy predchádzajúcich aktivít	Testovacie scenáre a testovacie prípady používateľského akceptačného testovania (UAT), Protokol o ukončení používateľských akceptačných testov (UAT)	28.6.2021	30.06.2021	Príprava a vykonanie integračných testov	Projektový manažér, Test manažér
Zavedenie do prevádzky v produkčnej infraštruktúre, monitoring	Výstupy predchádzajúcich aktivít	Dohoda o úrovni poskytovaných služieb (SLA) a manažment post implementačných zmien, Akceptačný protokol o zavedení komponentov a integrácie do produkčného prostredia	01.07.2021	01.07.2021	Príprava a vykonanie používateľských akceptačných testov (UAT)	Projektový manažér
Implementácia papierovej cesty	Implementácia do tenkých klientov na pobočky	Protokol o ukončení používateľských akceptačných testov (UAT)	N/A - Nebude začaté do schválenia legislatívy, ktorá umožní spracovanie dát v súlade s GDPR		Schválená legislatíva v súlade s GDPR	

4.2 Nevyhnutné podmienky

Nevyhnutnými podmienkami integrácie subjektov pre naplnenie účelu Dohody sú:

- dostupné API SCA na strane NCZI vo všetkých prostrediach
- dostupná integračná platforma a back-office systémy na strane NCZI
- dostupná technická špecifikácia poskytovaných služieb SCA (popis API, certifikáty a pod.)
- Platná legislatíva umožňujúca NCZI vydávanie a poskytovanie údajov o DGC pre DZP

4.3 Externé závislosti

Nie sú.

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, daňový poradcovia, audítori), 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 podmienkami uvedenými v tejto Dohode.
4. 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 Spracúvanie osobných údajov a záruky za ochranu osobných údajov

1. Subjekty Dohody majú pri plnení účelu tejto Dohody postavenie samostatných prevádzkovateľov podľa GDPR.
2. Právnym základom poskytnutia osobných údajov medzi samostatnými prevádzkovateľmi je splnenie zákonnej povinnosti alebo plnenie úlohy realizovanej vo verejnom záujme podľa čl. 6 ods. 1 písm. c) alebo e) GDPR a v prípade údajov o zdraví aj za splnenia podmienky podľa čl. 9 ods. 2 písm. b), g) a/alebo i) GDPR, a to podľa znenia príslušných právnych predpisov.
3. Pre účely plnenia predmetu tejto Dohody budú zmluvné strany ako samostatní prevádzkovatelia spracúvať osobné údaje poistencov iba v minimálnom rozsahu, ktorý je nevyhnutný pre splnenie účelu spracúvania. Rozsah osobných údajov je stanovený v Nariadení o DCC.
4. Účelom spracovania osobných údajov dotknutých osôb je v prípade NCZI sprístupňovanie certifikátov DZP. DZP spracúva osobné údaje za účelom plnenia zákonnej povinnosti pri vykonávaní verejného zdravotného poistenia - sprístupnenia certifikátov poistencom, a to po dobu, po ktorú bude trvať účel spracúvania, t. j. pokiaľ bude potrebné sa preukazovať certifikátom na území Slovenskej republiky alebo inom členskom štáte EÚ. Po skončení obdobia uplatňovania Nariadenia o DCC nesmie dôjsť k žiadnemu ďalšiemu spracúvaniu.¹
5. Kategórie dotknutých osôb sú poistenci DZP, ktorí boli na Slovensku očkovaní vakcínou proti ochoreniu COVID-19 alebo podrobení testu NAAT a/alebo rýchlemu antigénovému testu alebo ktorí prekonali ochorenie COVID-19. Zmluvné strany budú spracúvať aj osobitnú kategóriu osobných údajov – údaje týkajúce sa zdravia.
6. DZP si je vedomá toho, že nie je oprávnená osobné údaje spracúvať na žiadne ďalšie účely spracúvania a nebude ich poskytovať žiadnym tretím stranám (ďalším prevádzkovateľom), pokiaľ to príslušní právne predpisy nebudú stanovovať inak.
7. Subjekty Dohody sa zväzujú v súvislosti s plnením účelu tejto Dohody spracúvať osobné údaje dotknutých osôb za každých okolností v súlade s platnými a účinnými právnymi predpismi, predovšetkým GDPR a každý zo subjektov Dohody plne a samostatne zodpovedá za zákonné spracúvanie týchto osobných údajov, ak príslušný právny predpis neustanovuje inak.
8. NCZI sa zaväzuje vo svojich informačných povinnostiach podľa čl. 13/14 GDPR informovať dotknuté osoby o tom, že ich osobné údaje budú poskytované DZP ako príjemcovi. DZP sa zaväzuje informovať v súlade s čl. 13/14 GDPR všetky dotknuté osoby (príjemcov) o spracúvaní ich osobných údajov, ktoré

¹ Čl. 10 ods. 2 Nariadenia o DCC.

- vykonáva DZP, vrátane informácie o tom, že zdrojom certifikátov a predmetných osobných údajov je NCZI.
9. DZP sa zaväzuje ukončiť sprístupňovanie certifikátov a osobných údajov ak to príslušné právne predpisy stanovujú alebo po tom, čo o to NCZI požiada na základe právne zdôvodnenej žiadosti, najmä z dôvodu ohrozenia bezpečného spracovania osobných údajov (bezpečnostný incident). DZP je povinné bezodkladne opraviť, upraviť, obmedziť alebo vymazať poskytnuté osobné údaje, ak o to NCZI požiada na základe právne zdôvodnenej žiadosti.
 10. Žiadosti dotknutých osôb podľa GDPR vybavuje každá zmluvná strana samostatne a len v rozsahu, v ktorom daná zmluvná strana spracúva osobné údaje ako prevádzkovateľ.
 11. Pre vylúčenie akýchkoľvek pochybností, od momentu sprístupnenia certifikátu DZP spôsobom dohodnutom v tejto zmluve nesie DZP plnú zodpovednosť za sprístupnené certifikáty a údaje v nich obsiahnuté.
 12. Pre vylúčenie všetkých pochybností subjekty Dohody konštatujú, že ustanovenia tohto článku Dohody sa týkajú spracúvania iba tých osobných údajov, ktoré subjekty Dohody spracúvajú na právnych základoch a za účelmi uvedenými v tejto Dohode a súčasne ide o osobné údaje sprístupnené od NCZI pre DZP; týmto nie sú dotknuté práva a povinnosti subjektov Dohody podľa GDPR v súvislosti so spracúvaním iných osobných údajov v súvislosti s touto Dohodou.
 13. Subjekty Dohody sa zaväzujú osobitne zabezpečiť technický prenos spracúvaných osobných údajov zo systémov NCZI do systémov DZP prijatím vzájomne dohodnutých funkčných technických a organizačných opatrení garantujúcich primeranú ochranu pred neoprávneným narušením dôvernosti, dostupnosti a integrity osobných údajov počas ich technického prenosu cez verejne prístupnú počítačovú sieť, pričom bližšie podrobnosti sú dohodnuté v tejto Dohode. Za bezpečnosť spracúvania osobných údajov zodpovedá každý subjekt Dohody samostatne ako prevádzkovateľ vo vzťahu k vlastným informačným systémom, v ktorých sa spracúvajú osobné údaje. Bezpečnosť spracúvania osobných údajov počas technického prenosu osobných údajov zo systémov spravovaných NCZI do informačného systému DZP sa spravuje touto Dohodou.
 14. Subjekty tejto Dohody sa zaväzujú, že osobné údaje budú spracovávané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.
 15. Subjekty tejto Dohody vyhlasujú, že poskytujú dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky právnych predpisov o ochrane osobných údajov a aby sa zabezpečila ochrana práv dotknutej osoby.
 16. DZP vyhlasuje, že poskytnutím osobných údajov zo systémov NCZI do informačného systému DZP NCZI nevykoná cezhraničný prenos osobných údajov do tretej krajiny nezabezpečujúcej primeranú úroveň ochrany osobných údajov.
 17. Subjekty Dohody sa zaväzujú spolupracovať a poskytovať si maximálnu súčinnosť v prípade akýchkoľvek konaní alebo kontrol týkajúcich sa spracúvania osobných údajov na účely podľa tejto Dohody vedených Úradom na ochranu osobných údajov Slovenskej republiky, súdmi alebo inými orgánmi, ako aj v prípade vzniku závažných bezpečnostných incidentov a porušení ochrany osobných údajov zasahujúcich technické prenosy osobných údajov od NCZI do informačného systému DZP pri spolupráci podľa tejto Dohody, a to bez ohľadu na začatie konania alebo kontroly príslušného dozorného orgánu. Akékoľvek konania alebo kontroly v tejto súvislosti sú si subjekty Dohody povinné vzájomne oznamovať.
 18. Subjekt Dohody, ktorý zistil závažný bezpečnostný incident alebo porušenie ochrany osobných údajov, je povinný najneskôr do 24 hod od jeho zistenia informovať druhý subjekt Dohody s ohľadom na všetky dostupné informácie týkajúce sa povahy zisteného bezpečnostného incidentu alebo porušenia ochrany osobných údajov, pričom sa poskytujú najmä informácie podľa čl. 33 ods. 3 GDPR pre prípad porušenia ochrany osobných údajov a podľa § 24 ods. 4 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v spojitosti s § 2 ods. 1 a 2 vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z. Národného bezpečnostného úradu, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov pre prípad závažných bezpečnostných incidentov.
 19. Zodpovedné osoby subjektov Dohody, ktoré sú oprávnené samostatne komunikovať záležitosti subjektov Dohody týkajúce sa osobných údajov, sú:
 - a) za DZP:
 - b) za NCZI:

7 Záverečné ustanovenia

1. Táto Dohoda je vyhotovená v 2 vyhotoveniach, z ktorých jedno (1) vyhotovenie obdrží DZP a jedno (1) vyhotovenie NCZI. Táto Dohoda nadobúda platnosť dňom jej podpísania oprávnenými zástupcami – oboch subjektov Dohody a účinnosť nasledujúci deň po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky. Zverejnenie tejto Dohody v registri sa nepovažuje za porušenie mlčanlivosti.
2. Táto Dohoda sa uzatvára na dobu uplatňovania Nariadenia o DCC.
3. Túto Dohodu je možné meniť a dopĺňať len písomnou dohodou oboch subjektov Dohody vo forme očíslovaných dodatkov.
4. Dohodu je možné ukončiť písomnou dohodou oboch subjektov Dohody, alebo písomnou výpoveďou ktoréhokoľvek subjektu Dohody aj bez uvedenia dôvodov. Výpovedná lehota je dva mesiace a začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola doručená písomná výpoveď druhému subjektu Dohody na adresu sídla uvedenú v záhlaví tejto Dohody.
5. 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.
6. Oprávnení zástupcovia 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.