Dohoda o integračnom zámere Ministerstva obrany Slovenskej republiky a Národného centra zdravotníckych informácií

Subjekt	Národné centrum zdravotníckych informácií	**Subjekt**	Ministerstvo obrany Slovenskej republiky
Meno	Mgr. Pavol Vršanský	**Meno**	plk. Ing. Štefan ČAHOJ
Funkcia	riaditeľ	**Funkcia**	riaditeľ OdRSaPKIS SEMOD – poverený správca Integrovaného informačného systému IIS MO SR.
Dátum		**Dátum**	
Podpis		**Podpis**	

Projekt:	Integrácia za účelom elektronizácie procesu dočasných pracovných neschopností.
Dokument:	DIZ_NCZI_eZdravie MO SR
Verzia:	1.6
Dátum:	18.12.2024
Autor:	[redacted]
Vlastník:	Národné centrum zdravotníckych informácií

História dokumentu

1.0	NCZI	DIZ na pripomienkovanie MO SR	15.11.2024
1.1	MOSR	Pripomienky zo strany MOSR	28.11.2024
1.2	NCZI	Zapracovanie pripomienok - finálna verzia DIZ	06.12.2024
1.3	NCZI	Príloha č. 1 – kód MOSR - aktualizácia, úprava legislatívy	09.12.2024
1.4	NCZI	Pripomienky právneho odboru, DPO NCZI	13.12.2024
1.5	NCZI	Zapracovanie pripomienok,	17.12.2024
1.6	NCZI	Zapracovanie pripomienok, Odsúhlasenie MOSR	18.12.2024

Obsah

Skratky

DIZ alebo Dohoda	Dohoda o integračnom zámere
DPN	Dočasná práce neschopnosť
ePN	Elektronická práce neschopnosť
ETL	extract, transform, load
GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 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)
IS-MOSR	Informačný systém Ministerstva obrany Slovenskej republiky pre spracovanie údajov týkajúcich sa nemocenského zabezpečenia
IS PZS	Informačný systém poskytovateľa zdravotnej starostlivosti
MOSR	Ministerstvo obrany Slovenskej republiky
NCZI	Národné centrum zdravotníckych informácií
NRSR	Národná rada Slovenskej republiky
NZIS	Národný zdravotnícky informačný systém
PZS	Poskytovateľ zdravotnej starostlivosti
SP	Sociálna poisťovňa
SZ	Silová zložka
SD	Service desk – nástroj na evidenciu a riešenie problémov s informačnými systémami
SFTP	Secure File Transfer Protocol
VS platiteľa	Identifikátor osoby zaslaný príslušným úradom
VS príjemcu	Variabilný symbol (kódový identifikátor silovej zložky)
XSD	XML Schema Definition
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
ZoNZIS	Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

1 Úvodné ustanovenia

1.1 Identifikácia subjektov integračného zámeru

Subjektmi Dohody o integračnom zámere sú Národné centrum zdravotníckych informácií (NCZI) a Ministerstvo obrany Slovenskej republiky Konzumentom riešenia v rámci integrácie bude IS-MOSR, poskytovateľom riešenia bude NZIS

Subjekty Dohody	Rola	Správca (Gestor)	ISVS spadajúce pod Dohodu
	Konzument	Ministerstvo obrany Slovenskej republiky, so sídlom: Námestie generála Viesta 2, 832 47 Bratislava IČO: 30845572	IS-MOSR
	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.

Elektronizácia práceneschopnosti a súvisiacich nemocenských dávok prebehla v roku 2022, kedy od 1.6.2022 Sociálna poisťovňa začala prijímať záznamy o potvrdení práceneschopnosti lekárom elektronicky. Lekár najprv zapisuje záznam prostredníctvom svojho IS do NZIS, následne bol záznam preposlaný na Sociálnu poisťovňu, ktorá ho ďalej spracovala a vyhodnotila nárok na dávku. Od augusta 2022 sa do systému postupne zapojili aj tzv. silové rezorty SR, pričom NZIS bol rozšírený o rozhodovanie na ktorú inštitúciu je potrebné záznam ePN smerovať.

Ministerstvo obrany SR ako jeden zo silových rezortov dostáva záznamy ePN svojich ozbrojených príslušníkov, teda tých, ktorých poistiteľom je samotný silový rezort a ktorý im počas práceneschopnosti vypláca nemocenskú dávku. Okrem silových príslušníkov je MOSR zamestnávateľ aj civilných zamestnancov, ktorých poistiteľom je Sociálna poisťovňa, kde ePN týchto zamestnancov sú spracovávané cez webové rozhranie Sociálnej poisťovne.

Na začiatku roka 2024 Ministerstvo obrany Slovenskej republiky vyjadril na spoločnom rokovaní s NCZI požiadavku, aby v pozícii zamestnávateľa cez existujúce rozhranie dostávali aj ePN civilných zamestnancov.

Povinnosť NCZI posielať ePN civilných zamestnancov MOSR je zakotvená aj v pripravovanej novele ZoNZIS.

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

1.3 Rozpočet

V súvislosti s navrhovanou právnou úpravou pre zabezpečenie potreby zasielania ePN civilných zamestnancov MO SR sú zapracované v analýze vplyvov na rozpočet verejnej správy v doložke vplyvov v ZoNZIS refundované MO SR vo výške 39 234,00 eur - kapitálový transfer.

2 Rozsah integrácie

Rozsah kompletnej integrácie NZIS a IS-MOSR je definovaný v ustanovení § 3a ods. 28 písm. c) ZoNZIS v znení zákona č. 361/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

V prípade potreby zmeny rozsahu integrácie sa táto Dohoda upraví dodatkom.

2.1 Procesy IS z pohľadu komunikácie voči NZIS

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.

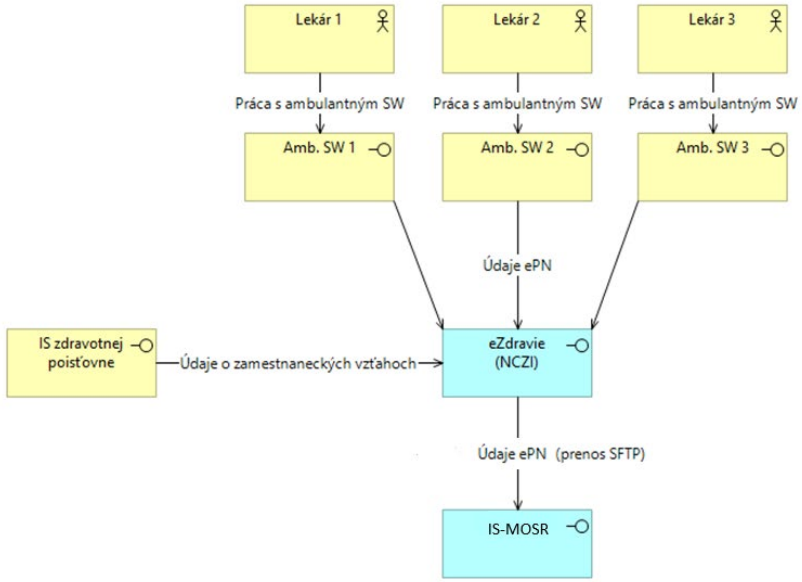
Pozn.: Lekár má okrem údajov o fyzickej osobe v prípade poistencov silových rezortov aj informáciu o tom, že sú poistencami silových rezortov, bez bližšej špecifikácie.

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 do MOSR na definované rozhranie IS MOSR, šifrovane. Popis šifrovania v prílohe č. 1.

Oprávnený ošetrujúci lekár posudzuje práce(ne)schopnosť pacienta. Zodpovednosť má PZS. NCZI zabezpečí, aby tento proces umožnil realizovať IS PZS voči NZIS.

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



Z pohľadu MOSR 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 SP, vrátane poskytnutia údajov z registra zamestnávateľských vzťahov lekárom.
2. IS-MOSR – informačný systém na strane MOSR pre spracovanie údajov týkajúcich sa nemocenského zabezpečenia.

2.2 Popis hlavných služieb využívaných v procesoch

Podrobný popis služieb, ktoré sú predmetom tejto integrácie sú uvedené v prílohe č. 1.

2.3 Údaje o využívaní služby

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

V prípade vyžiadania MO SR, NCZI dodá požadované informácie z log súborov z ich časti systému v danom rozsahu najneskôr do 15 dní od výzvy MOSR. 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.

2.4 Riešenie chýb a incidentov

Pre riešenie chýb a výpadkov je stanovený nasledujúci postup:

Možné chybové stavy v spracovaní:

1. Ak endpoint MOSR nemá vytvorený alebo dostupný podadresár pre daného adresáta („VS“) a nie je možné ho vytvoriť pred nahraním súboru, bude súbor 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. exspirovaná 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 zaslanej e-mailovej notifikácie z SD.

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

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

2.5 Metodika integrácie

Integrácia IS-MOSR bude realizovaná v súlade s dokumentom „*Metodika integrácie informačného systému* “ „*Metodika integrácie informačného systému*“, ktorý je podľa § 9 ods. 5 Zákona o NZIS dostupný na webovom sídle NCZI (https://www.ezdravotnictvo.sk/documents/1005903/1007442/Metodika_integracie_informacneho_systemu.pdf).“

2.6 Overenie zhody a testovacie scenáre

Proces overenia zhody nie je požadovaný v zmysle danej integrácie podľa § 11 zákona č. ZoNZIS. Testovanie prebehne na základe UAT testov (kontrola maskovania údajov pre MOSR).

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	MO SR	Poskytovateľ NCZI
Projektový manažér /Produktový manažér	[redacted]	[redacted]
Integračný manažér	[redacted]	[redacted]

3.2 Komunikačné procesy

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

Úroveň stretnutí	Komunikačný proces	Výstup
Integračný /Projektový manažéri	Návrh integračného zámeru a jeho úprav	Dohoda o integračnom zámere a jeho dodatok
Integračný /Projektový manažéri	Eskalácia problémov	Elektronický alebo papierový výstup k eskalácii problému
Integračný /Projektový manažéri	Monitorovanie stavu integračných prác	Zápis zo stretnutia

4 Harmonogram

4.1 Popis harmonogramu

Aktivita	Vstup	Výstup	Dátum začiatku	Dátum Ukončenia	Zodpovedná osoba
Vypracovanie integračnej dokumentácie	Integračný manuál, Integračný zámer	Integračný manuál poskytovanej služby,	15.11.2024	20.12.2024	Integračný manažér
Nasadenie IS do Produkcie	UAT testy	Protokol z UAT testov	01.01.2025	01.01.2025	Integračný manažér MOSR

4.2 Nevyhnutné podmienky

Nevyhnutnými podmienkami integrácie subjektov pre naplnenie Dohody sú:

- dostupné webové služby (WS) NZIS na strane NCZI vo všetkých prostrediach
- dostupná integračná platforma a back-office systémy na strane NCZI
- vytvorenie technických prihlasovacích údajov pre údajovú základňu NZIS
- PKI infraštruktúra pre autorizáciu
- dostupná technická špecifikácia poskytovaných služieb NZIS (WSDL, XSD schémy)
- nahlásené aktuálne údaje o právnych vzťahoch a výkone povolania poverených osôb zo strany MOSR v zmysle ustanovení ZoNZIS a v súčinnosti s ustanoveniami zákona 578/2004 Z. z. o

poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov,

4.3 Externé závislosti

Žiadne

5 Mlčanlivosť a ochrana dôverných informácií

1. Subjekty tejto Dohody sa zaväzujú zachovávať mlčanlivosť o akýchkoľvek informáciách, materiáloch, dokumentácii poskytnutých resp. získaných v súvislosti s touto Dohodou ako aj s informáciami majúcimi charakter osobných údajov (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), 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 zaviazať 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 po tom, čo sa o takomto porušení dozvie. Porušujúca strana – subjekt tejto Dohody je povinná bezodkladne vykonať opatrenia na zamedzenie porušovania povinnosti mlčanlivosti.
5. Spracúvanie osobných údajov podľa tejto Dohody sa riadi zákonmi a ostatným všeobecne záväznými právnymi predpismi platnými a účinnými v čase spracúvania osobných údajov na území Slovenskej republiky.
6. Za bezpečnosť poskytovaných osobných údajov zodpovedá každý subjekt Dohody od ich preukázateľného prevzatia až do okamihu ich preukázateľného odovzdania.
7. Subjekty dohody sa zaväzujú využívať údaje, ktoré si vzájomne poskytujú v súlade s touto Dohodou, len na účely stanovené v tejto Dohode, neposkytnúť a nesprístupniť ich tretím stranám, nespracovať ich na iný účel a nezverejňovať žiadnym spôsobom, pokiaľ všeobecne záväzný právny predpis neustanovuje inak.
8. Subjekty Dohody sú povinné v súlade s GDPR a/alebo ZoOOU 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.
9. Ochrana osobných údajov podľa dohody trvá aj po ukončení zmluvného vzťahu založeného touto Dohodou a zaväzuje aj právnych nástupcov subjektov dohody. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá subjektu dohody vznikla porušením povinností zo strany druhého subjektu dohody.

10. Neoddeliteľnou súčasťou tejto Dohody je príloha č. 2 Poučenie o ochrane osobných údajov pri ich spracúvaní v informačných systémoch, ktorého obsah zaväzuje subjekty Dohody.

6 Bezpečnosť

1. MOSR ako integrujúca sa organizácia sa zaväzuje dodržiavať všetky požiadavky na bezpečnosť definované všeobecne záväznými právnymi predpismi, najmä ZoKB a ZoITVS a súvisiacich vyhlášok. Zároveň sa zaväzuje chrániť všetky osobné údaje v zmysle GDPR a ZoOOU.
2. MO SR je povinné bezodkladne hlásiť identifikované bezpečnostné incidenty alebo narušenia bezpečnosti súvisiacej s informačnými technológiami používanými pre získavanie údajov z prostredia NCZI a bezodkladne oznámiť všetky skutočnosti, ktoré by mohli zapríčiniť narušenie bezpečnosti rozhrania alebo informačného systému NCZI pre poskytovanie služby NZIS na kontaktnú adresu (csirt@nczisk.sk) a zabezpečiť súčinnosť pre NCZI v rámci riešenia incidentu.
3. MOSR sa zväzuje zabezpečiť:
    a) znemožnenie prístupu neoprávneným osobám k dátam NZIS
    b) používanie certifikátov v súlade s certifikačným poriadkom NCZI,
    c) šifrovanú komunikáciu medzi IS-MOSR a NCZI,
    d) pravidelný dohľad využitia komunikácie medzi IS-MOSR a NCZI a identifikáciu neštandardného správania používateľov IS MOSR.

7 Záverečné ustanovenia

1. Táto Dohoda nadobúda platnosť dňom podpisu oprávnenými zástupcami subjektov Dohody a **účinnosť dňom 01.01.2025**, a to za súčasného splnenia podmienky predchádzajúceho zverejnenia Dohody v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky (ďalej len „**register**“). Zverejnenie tejto Dohody v registri sa nepovažuje za porušenie mlčanlivosti. Zverejnenie tejto Dohody v registri sa nepovažuje za porušenie mlčanlivosti. Subjekty tejto Dohody sa zároveň dohodli, že z dôvodov uvedených v ust. § 5a ods. 4 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov nezverejňujú nasledovnú prílohu Dohody: príloha č. 1 (Technická špecifikácia).
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.

8 Prílohy:

Príloha č. 1: Technická špecifikácia
Príloha č. 2: Poučenie o ochrane osobných údajov pri ich spracovaní v informačných systémoch

POUČENIE O OCHRANE OSOBNÝCH ÚDAJOV PRI ICH SPRACÚVANÍ V INFORMAČNÝCH SYSTÉMOCH

ZHRNUTIE ZÁKLADNÝCH INFORMÁCIÍ

V súčasnosti sú účinné dva základné právne predpisy určené na ochranu osobných údajov: 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 (všeobecné nariadenie o ochrane údajov, ďalej v texte aj ako „**GDPR**“) a Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej v texte aj ako „**zákon č. 18/2018 Z. z.**“). Postavenie a úlohy Národného centra zdravotníckych informácii (ďalej len „NCZI“), údajovú základňu národného zdravotníckeho informačného systému a aj aspekty spracúvania a sprístupňovania údajov (vrátane osobných údajov) upravuje Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov (ďalej v texte aj ako „**zákon č. 153/2013 Z. z.**“).

Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, pričom identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Údaje týkajúce sa zdravia sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave. Údaje týkajúce sa zdravia sú citlivé osobné údaje, ktoré majú podľa právnych predpisov na ochranu osobných údajov vyššiu mieru ochrany. NCZI spracúva údaje týkajúce sa zdravia vo veľmi veľkom rozsahu.

Naintegrovaná organizácia, ktorá spracúva osobné údaje dotknutých osôb získané z registrov NCZI má viacero povinností, a to najmä:

- aplikovať základné zásady spracúvania osobných údajov (zásada správnosti, zásada minimalizácie uchovávania, zásada integrity a správnosti, zásada obmedzenia účelu a ďalšie);
- povinnosť informovať dotknuté osoby o ich právach (právo na vymazanie, právo namietať spracúvanie, právo na opravu a ďalšie) ako aj spôsobe ich uplatnenia;
- povinnosť implementovať primerané technické a organizačné bezpečnostné opatrenia a vedieť splnenie uvedenej povinnosti preukázať;
- kontrolovať dodržiavanie povinností a zásad ochrany osobných údajov zo strany všetkých fyzických osôb, ktoré spracúvajú osobné údaje z jej poverenia (napr. zamestnanci);
- povinnosť realizovať posudzovanie rizík pre práva a slobody fyzických osôb v kontexte spracúvania osobných údajov v informačných systémoch a povinnosť vykonať posúdenie vplyvu na ochranu údajov, ak typ spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb.

Právne predpisy kladú dôraz aj na dodržiavanie a kontrolu jednotlivých povinností fyzických osôb konajúcich na základe poverenia naintegrovanej organizácie (tzv. oprávnené osoby, ktoré majú prístup k osobným údajom dotknutých osôb). Naintegrovaná organizácia je povinná oprávnené osoby poučiť o ich povinnostiach vyplývajúcich z právnych

predpisov na ochranu osobných údajov. Medzi minimálne základné povinnosti oprávnených osôb, ktoré sa podieľajú na spracúvaní osobných údajov (napr. zamestnanci), patria najmä nasledovné:

- povinnosť spracúvať osobné údaje dotknutých osôb výlučne a len na účel a v rozsahu ako bol vymedzený a stanovený naintegrovanou organizáciou;
- povinnosť realizovať spracovateľské operácie len so správnymi, úplnými a aktualizovanými osobnými údajmi dotknutých osôb;
- chrániť osobné údaje, ako aj všetky dokumenty (elektronické a/alebo listinné) obsahujúce osobné údaje dotknutých osôb pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými alebo nezákonnými formami spracúvania;
- dodržiavať povinnosť mlčanlivosti o všetkých osobných údajoch, s ktorými osoba spracúvajúca osobné údaje (napr. zamestnanci) prichádza v rámci svojho pracovnoprávneho vzťahu (alebo funkčného zaradenia) alebo iného vzťahu k naintegrovanej organizácii do kontaktu, a to aj po zániku tohto vzťahu;
- v prípade bezpečnostného incidentu alebo porušenia ochrany osobných údajov bezodkladne informovať o tejto skutočnosti zodpovednú osobu (DPO) alebo iného príslušného zamestnanca prevádzkovateľa.

ROZDIELY V UPLATŇOVANÍ POSTUPOV PODĽA GDPR A PODĽA ZÁKONA

(1) Ak pôjde o spracúvanie osobných údajov v rámci činnosti naintegrovanej organizácie, ktorá spadá pod právo Únie, bude sa na organizáciu vzťahovať GDPR, uplatňovať sa ale bude aj zákon č. 18/2018 Z. z., a to s výnimkou jeho 2. a 3. časti; teda zo zákona č. 18/2018 Z. z. bude pre naintegrovanú organizáciu relevantná prvá časť okrem § 2 a § 5 a následne štvrtá až šiesta časť zákona č. 18/2018 Z. z.

(2) Ak pôjde o spracúvanie osobných údajov v rámci činnosti naintegrovanej organizácie, ktoré nespadá pod právo Únie a prevádzkovateľom nie je príslušný orgán, uplatňovať sa bude zákon č. 18/2018 Z. z. okrem jeho tretej časti.

(3) V prípade spracúvania osobných údajov prevádzkovateľom v postavení príslušného orgánu tento bude postupovať pri spracúvaní osobných údajov fyzických osôb na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií podľa zákona č. 18/2018 Z. z. konkrétne jeho prvej časti a tretej až šiestej časti s ohľadom na niektoré ustanovenie z druhej časti.

FYZICKÉ OSOBY SPRACÚVAJÚCE OSOBNÉ ÚDAJE - VŠEOBECNE

GDPR a zákon č. 18/2018 Z. z. explicitne určujú naintegrovanej organizácii povinnosť určiť osoby, ktoré budú poverené spracúvaním osobných údajov a zároveň určiť týmto osobám podmienky tohto spracúvania osobných údajov. V rámci zákona č. 18/2018 Z. z. a rovnako aj v rámci GDPR je v tejto súvislosti zavedený a používaný všeobecný termín „fyzické osoby konajúce za prevádzkovateľa alebo sprostredkovateľa, ktoré majú prístup k osobným údajom[1]“. Pre účely zjednodušenia výkladu bude v ďalšom texte v tejto súvislosti používaný pojem „osoby poverené spracúvaním osobných údajov“ alebo „osoby spracúvajúce osobné údaje“.

V tejto súvislosti je rovnako potrebné zdôrazniť aj znenie **čl. 32 ods. 4 GDPR**, na základe ktorého „Prevádzkovateľ a sprostredkovateľ podniknú kroky na zabezpečenie toho, aby každá fyzická osoba konajúca na základe poverenia prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, **spracúvala tieto údaje len na základe pokynov prevádzkovateľa** s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Únie alebo práva členského

[1] Pozri. § 39 ods. 4 zákona č. 18/2018 Z. z.

štátu“[2]. Citované ustanovenie znamená, že naintegrovaná organizácia je povinná podniknúť všetky potrebné kroky na usmernenie činnosti osôb, ktoré pre ňu a v jej mene spracúvajú osobné údaje dotknutých osôb.

Osoba poverená spracúvaním osobných údajov má právo vykonávať spracovateľské operácie s osobnými údajmi spracúvanými v príslušných informačných systémoch výlučne **v súlade s konkrétne stanoveným právnym základom, od ktorého naintegrovaná organizácia odvodzuje jeho oprávnenie spracúvať osobné údaje dotknutých osôb a zároveň len v rozsahu a spôsobom, ktorý je nevyhnutný na dosiahnutie vymedzeného účelu spracúvania** a ktorý je v súlade so zákonom č. 18/2018 Z. z., GDPR, inými všeobecne záväznými právnymi predpismi a/alebo internými normatívnymi aktmi naintegrovanej organizácie.

ZODPOVEDNOSŤ ZA PORUŠENIE PRÁV DOTKNUTEJ OSOBY ALEBO POVINNOSTÍ SÚVISIACICH S OCHRANOU OSOBNÝCH ÚDAJOV

Porušenie povinností, súvisiacich s ochranou osobných údajov (napr. porušenie zásad ochrany osobných údajov zo strany osoby spracúvajúcej osobné údaje), môže v konečnom dôsledku viesť až k uloženiu administratívnej pokuty za delikty v zmysle § 104 zákona č. 18/2018 Z. z[3]. V dôsledku uvedeného môže zamestnávateľ (naintegrovaná organizácia, ktorej bola uložená pokuta) vyvodiť voči takejto osobe pracovnoprávnu zodpovednosť za škodu pri výkone práce alebo v súvislosti s ňou v zmysle zákona č. 311/2001 Z. z. Zákonníka práce (v rozsahu všeobecnej zodpovednosti zamestnanca za škodu spôsobenú zamestnávateľovi).

Nezákonné konanie osoby, ktorá spracúva osobné údaje dotknutých osôb (osoba poverená spracúvaním) môže, v súvislosti so spracúvaním osobných údajov viesť v niektorých prípadoch až k naplneniu skutkovej podstaty trestných činov podľa § 247, § 247a, § 247b, a/alebo § 374 zákona č. 300/2005 Z. z. Trestného zákona v znení neskorších predpisov.

POUČENIE O POVINNOSTIACH PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Prílohou tohto poučenia je aj **Poučenie o povinnostiach pri spracúvaní osobných údajov**.

[2] Analogicky § 39 ods. 4 zákona č. 18/2018 Z. z.

[3] Pri porušení povinností podľa § 104 ods. 2 zákona č. 18/2018 Z. z. až do výšky 20 000 000 EUR alebo ak ide o podnik do 4 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.

Príloha: Poučenie o povinnostiach pri spracúvaní osobných údajov

I. **Národné centrum zdravotníckych informácii,** so sídlom Lazaretská 26, 811 09 Bratislava 1 IČO: 00165387 (ďalej len ako „**NCZI**“) a

II. **Tretia strana,** ktorej sú poskytované osobné údaje (ďalej len ako „**Príjemca**“ alebo “**Naintegrovaná organizácia**”).

ČLÁNOK I PRÍSTUP PRÍJEMCU K OSOBNÝM ÚDAJOM

1. Vzhľadom na povahu činnosti NCZI a potrebu NCZI naintegrovať Príjemcu do informačného systému NCZI, realizuje Prevádzkovateľ aj poučenie o povinnostiach pri spracúvaní osobných údajov (ďalej len „**Poučenie**“).

2. Príjemca má prístup k osobným údajom, ktorých prevádzkovateľom je NCZI.

3. Prístup k osobným údajom je možný len na základe objektívnej potreby plnenia zákonných povinností a pracovných úloh Príjemcu. Prístup k osobným údajom je kontrolovaný a prebieha na základe pridelenia prístupových práv k príslušným systémom, resp. prostriedkom spracúvania osobných údajov v súlade s internými postupmi NCZI.

4. Príjemca je povinný pri spracúvaní osobných údajov dodržiavať rozsah pridelených prístupových práv a rolí, ktoré sú mu pridelené zo strany NCZI.

ČLÁNOK II ZÁKLADNÉ POVINNOSTI PRÍJEMCU

1. Príjemca je povinný pri vykonávaní spracovateľských operácií dodržiavať právne predpisy na ochranu osobných údajov, najmä GDPR a zákon č. 18/2018 Z. z. a zákon č. 153/2013 Z. z.

2. NCZI je oprávnené vydať Príjemcovi ďalšie pokyny, ktoré sú pre Príjemcu záväzné, ak sú také pokyny nevyhnutné na zabezpečenie súladu NCZI s GDPR, Zákonom č. 18/2018 Z. z. a Zákonom č. 153/2013 Z. z. Interné predpisy stanovujú, ktoré ďalšie osoby sú v rámci NCZI oprávnené udeliť Príjemcovi ďalšie záväzné pokyny týkajúce sa ochrany osobných údajov, a to najmä DPO Prevádzkovateľa.

3. Príjemca nesmie vykonávať s osobnými údajmi spracúvanými NCZI žiadne neoprávnené spracovateľské operácie v zmysle čl. 4 bodu 2 GDPR, najmä nesmie osobné údaje neoprávnene poskytnúť, sprístupniť, zverejniť alebo k nim umožniť iný prístup akémukoľvek neoprávnenému príjemcovi a/alebo tretej strane. V prípade, ak tak Príjemca urobí, koná na svoju vlastnú zodpovednosť. Príjemca je oprávnený osobné údaje spracúvané v informačnom systéme spracúvať len zákonným spôsobom na účely spracúvania vyplývajúce zo zákona. Príjemca nesmie osobné údaje spracúvané v informačnom systéme využiť a/alebo akokoľvek použiť pre svoje vlastné/osobné potreby, ktoré sú odlišné od tých, ktoré vyplývajú zo zákona a/alebo použiť na ciele alebo v prospech, či potreby alebo dosahovanie cieľov akejkoľvek neoprávnenej tretej strany. V prípade, ak tak Príjemca urobí, koná na svoju vlastnú zodpovednosť.

4. Príjemca je pri akýchkoľvek pochybnostiach o správnosti, zákonnosti či bezpečnosti postupu súvisiaceho so spracúvaním osobných údajov povinný vopred kontaktovať DPO NZCI alebo jej zástupcu a vyžiadať si usmernenie pre ďalší postup v danej veci. Do prijatia preukázateľnej odpovede DPO NCZI je Príjemca povinný zdržať sa akéhokoľvek konania, ktoré by mohlo viesť k porušeniu ochrany osobných údajov a/alebo všeobecne záväzných právnych predpisov a/alebo príslušných interných predpisov NCZI týkajúcich sa ochrany osobných údajov.

5. V prípade, ak sa Príjemca dozvie o porušení ochrany osobných údajov (bezpečnostný incident – porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému

poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim), ktoré sú spracúvané v informačnom systéme, bezodkladne o tom informuje zodpovednú osobu DPO NCZI.

ČLÁNOK III POVINNOSŤ MLČANLIVOSTI

1. Príjemca je povinný zachovávať mlčanlivosť o všetkých osobných údajoch, s ktorými príde do styku počas spolupráce s NCZI. Táto povinnosť mlčanlivosti trvá aj po skončení spolupráce s NCZI.

2. Tento záväzok mlčanlivosti sa neuplatňuje iba v prípadoch podľa § 79 ods. 3 a ods. 4 zákona č. 18/2018 Z. z., tzn. ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov SR pri plnení jeho úloh.

ČLÁNOK IV ZODPOVEDNOSŤ PRÍJEMCU ÚDAJOV

1. Porušením povinností ustanovených Príjemcovi alebo iným zneužitím pridelených oprávnení a prístupových práv pri spracúvaní osobných údajov môže Príjemca naplniť skutkovú podstatu správnych deliktov podľa článku 83 ods. 4 písm. a) a článku 84 ods. 5 GDPR. NCZI si v závislosti od miery zavinenia a zodpovednosti za uloženie sankcie (správnej pokuty) v dôsledku porušenia povinností alebo zneužitia oprávnení Príjemcu môže nárokovať od Príjemcu regresnú náhradu škody spôsobenú v dôsledku uloženia pokuty a/alebo iného nápravného opatrenia zo strany dozorného orgánu.

2. Príjemca môže v súvislosti s protiprávnym nakladaním s osobnými údajmi čeliť aj trestnoprávnej zodpovednosti.