Zmluva
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Čl. I
Zmluvné strany

Prevádzkovateľ:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
V zastúpení:	Ing. Ľubomír Vážny, generálny riaditeľ
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA
IČO:	308 07 484
DIČ:	2020592332

(ďalej len „prevádzkovateľ)

a

Dodávateľ:	**DXC Technology Information Services Slovakia s.r.o.**
Sídlo:	Galvaniho 7 820 02 Bratislava 23
V zastúpení:	Ing. Martin Peluha, konateľ Zdenko Böhmer, konateľ
Zápis v registri:	vedenom Okresným súdom Bratislava I Oddiel: Sro, vložka číslo: 6562/B
Bankové spojenie:	Tatra banka, a.s.
IBAN:	SK37 1100 0000 0026 7602 0027
IČO:	31367569
DIČ:	2020318223
IČ pre DPH:	SK2020318223

(ďalej (ďalej len „dodávateľ“)

(spolu ďalej ako „zmluvné strany“)

Čl. II
Preambula

1. Prevádzkovateľ je podľa § 3 písm. l) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“) prevádzkovateľom základnej služby podľa § 3 písm. k) body 2 a 3 zákona o kybernetickej bezpečnosti. Dodávateľ je podľa § 19 ods. 2 zákona o kybernetickej

bezpečnosti dodávateľom, ktorý na základe zmlúv na výkon činností poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa.

2. Zmluvné strany majú spolu uzatvorené nasledujúce zmluvy na výkon činností:

- Zmluva o poskytovaní služieb technickej podpory a rozvoja pre Informačný systém nemocenského poistenia a lekárskej posudkovej činnosti a poskytovaní služieb technickej podpory pre licenčné softvérové vybavenie SYRIUS, č. 122-277/2019-BA, uzatvorenej podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov dňa 9. júla 2019, predmetom ktorej je technická podpora IS NP a LPČ, rozvoj IS NP a LPČ a technická podpora pre licenčné softvérové vybavenie SYRIUS.

- Zmluva o poskytovaní služieb technickej podpory pre Informačný systém finančného riadenia Sociálnej poisťovne, č. 79808-5/2019-BA, uzvretá podľa § 269 ods. 2 Obchodného zákonníka 31.12.2019, ktorej predmetom je poskytovanie služieb technickej podpory pre IS FRSP.

(ďalej len „zmluvy na výkon činností“).

3. Za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a § 8 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška“) zmluvné strany uzatvárajú túto zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „zmluva“).

Čl. III
Predmet zmluvy

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť pri prevádzke sietí a informačných systémov prevádzkovateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom (ďalej len „kybernetický incident“), ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania sietí a informačných systémov prevádzkovateľa, s prevádzkou ktorých priamo súvisí výkon činností dodávateľa na základe zmlúv na výkon činností.
2. Výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa, poskytovaných dodávateľom, umožňuje prevádzkovateľovi:
    - Požadovať služby technickej podpory IS NP a LPČ (APV SYRIUS) - služby aplikačnej podpory, riešenie servisných požiadaviek, súčinnosť pri riešení problémov súvisiacich s IS NP a LPČ, odstraňovanie vád (chýb) a riešenie incidentov, inštalácia opravných verzií IS NP a LPČ (APV SYRIUS)
    - Požadovať služby rozvoja IS NP a LPČ (APV SYRIUS) - implementácia legislatívnych zmien a implementácia požiadaviek Objednávateľa
    - Požadovať technickú podporu pre licenčné aplikačné programové vybavenie SYRIUS
    - Požadovať služby technickej podpory IS FRSP - riešenie hlásených incidentov, poskytovanie konzultácií, súčinnosť pri riešení problémov súvisiacich s IS FRSP, odstraňovanie vád (chýb)

Čl. IV
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné politiky prevádzkovateľa, ktoré tvoria prílohu č. 1 k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami prevádzkovateľa.
2. Dodávateľ súhlasí s tým, že bezpečnostné politiky prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov prevádzkovateľa.
3. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú súčasťou bezpečnostnej politiky prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a bezpečnostných politikách prevádzkovateľa. Dodávateľ vyhlasuje, že s bezpečnostnými opatreniami súhlasí.
4. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti.
5. Dodávateľ je povinný chrániť všetky informácie ku ktorým má prístup na základe zmlúv na výkon činností alebo tejto zmluvy, alebo ktoré mu boli poskytnuté zo strany prevádzkovateľa s tým, že všetci dotknutí zamestnanci dodávateľa, jeho subdodávateľov a/alebo iné tretie osoby, prostredníctvom ktorých dodávateľ poskytuje služby podľa zmluvy na výkon činnosti (ďalej len „tretia osoba“) sú povinní podpísať vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.
6. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá je aktuálna a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi.
7. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy minimálne v oblastiach podľa § 20 ods. 3 písm. c) a d) zákona o kybernetickej bezpečnosti v rozsahu podľa § 7, a § 8, vyhlášky a v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa.
8. Dodávateľ je povinný doručiť prevádzkovateľovi zoznam zamestnancov dodávateľa, subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa zmlúv na výkon činností a tejto zmluvy a ktorí budú mať prístup k informáciám prevádzkovateľa (ďalej len „Zoznam osôb“). Dodávateľ je povinný oznámiť prevádzkovateľovi každú zmenu v zozname osôb podľa tohto bodu a to elektronicky prostredníctvom Ústredného portálu verejnej správy (ďalej „UPVS“). Dodávateľ je povinný zabezpečiť, aby každá osoba uvedená v Zozname osôb, schválená oddelením bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa podpísala vyhlásenie o mlčanlivosti a zúčastnila sa na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností podľa prílohy č. 1
9. Dodávateľ je povinný písomne informovať prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom na účely plnenia tejto zmluvy.
10. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Čl. V
Okolnosti plnenia zmluvy

1. Pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.
2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.
3. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa podľa zmlúv na výkon činností. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania zmluvy na výkon činnosti.
4. Odplata za plnenie povinností dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom dodávateľovi podľa zmlúv na výkon činností a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Čl. VI
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

Dodávateľ je povinný v rámci prevencie kybernetických incidentov, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa, a tým na činnosť prevádzkovateľa:

a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez siete a informačné systémy dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa,

b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmlúv na výkon činností a tejto zmluvy alebo budú mať prístup k informáciám prevádzkovateľa,

c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,

d) sledovať hrozby týkajúce sa dodávateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,

e) predchádzať hrozbe vzniku kybernetických incidentov,

f) v prípade vzniku kybernetických incidentov, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,

g) prijímať od prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,

h) zasielať prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a

i) spolupracovať s prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa.

Čl. VII
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident prevádzkovateľovi spôsobom určeným prevádzkovateľom, ktorý je uvedený v bezpečnostnej politike, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Dodávateľ je povinný riešiť kybernetický incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení kybernetického incidentu na mieste, reakciou na kybernetický incident a podporou reakcií na kybernetický incident.
3. Pri riešení kybernetických incidentov je dodávateľ povinný na žiadosť prevádzkovateľa spolupracovať s prevádzkovateľom, Národným bezpečnostným úradom a Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického incidentu.
4. Dodávateľ je povinný oznámiť prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ je povinný v čase kybernetického incidentu zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho prevádzkovateľovi.
6. Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.
7. Po vyriešení kybernetického incidentu je dodávateľ na výzvu prevádzkovateľa v určenej lehote povinný predložiť prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „ochranné opatrenie“) na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom na návrhu nového ochranného opatrenia.
8. Po schválení ochranného opatrenia prevádzkovateľom je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť prevádzkovateľovi.
9. Dodávateľ je povinný informovať prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to elektronicky prostredníctvom UPVS.

Čl. VIII
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmlúv na výkon činností a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. Dodávateľ je najmä

povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa.
2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.
3. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

Čl. IX
Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí, a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov na základe zákona o kybernetickej bezpečnosti a tejto zmluvy.
2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
3. Prevádzkovateľ môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti prevádzkovateľa pri výkone auditu realizuje prevádzkovateľom poverená tretia osoba.
4. Dodávateľ je pri audite povinný spolupracovať s prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
5. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh a úseku kybernetickej bezpečnosti podľa tejto zmluvy.
6. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer vykonať u dodávateľa audit.
8. Vykonanie alebo nevykonanie auditu prevádzkovateľom nezbavuje zodpovednosti dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.
9. Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.
11. Dodávateľ je oprávnený preukázať splenie povinností implementovať bezpečnostné opatrenia pomocou platného certifikátu ISO27001:2013 vydaného akreditovanou autoritou.

Čl. X
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenie kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania kybernetických incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa mu predložiť uvedenú dokumentáciu.
4. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy najneskôr od 1.4.2020.
5. V prípade, ak dodávateľ plní zmluvu o výkone činností prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov pre prevádzkovateľa, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby prevádzkovateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subdodávateľov.
6. Všetky informácie, ktoré majú vplyv na plnenie práv a povinností uvedených v tejto zmluve sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na adresy uvedené v záhlaví tejto zmluvy, a zároveň elektronicky prostredníctvom UPVS.
7. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, dodávateľ zodpovedá za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky a za dôsledky a škodu vzniknutú v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu, v celom rozsahu. Prevádzkovateľ má nárok na preukázanú náhradu škody, pokuty alebo iné náklady, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov dodávateľa.
8. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.
9. Po ukončení tejto zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

Čl. XI
Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom UPVS, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti je: vedúci oddelenia bezpečnosti informačných systémov.
3. Kontaktná osoba dodávateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je: manažér zodpovedný za dodávku projektov a riešení.
4. Kontaktné osoby podľa bodov 2. a 3. tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme na adresu zmluvnej strany uvedenú v záhlaví tejto zmluvy alebo elektronicky prostredníctvom UPVS.

Čl. XII
Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií) a v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov s výnimkou prílohy č. 1.
2. Táto Zmluva nadobúda platnosť dňom jej podpísania zmluvnými stranami a účinnosť dňom nasledujúcim po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády SR.
3. Táto zmluva sa uzatvára na dobu určitú po dobu platnosti a účinnosti zmlúv na výkon činností definovaných v čl. II. Počas platnosti a účinnosti zmlúv na výkon činností je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane. Zrušenie tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto dohody a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do zrušenia tejto zmluvy.
4. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.
5. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd SR.
6. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve.
7. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek nezákonného, neplatného

alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.

8. Neoddeliteľnou súčasťou tejto zmluvy je:
   príloha č. 1 - Bezpečnostné politiky
9. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.
10. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V ..... dňa .....

Za prevádzkovateľa:

....
Ing. Ľubomír Vážny
generálny riaditeľ
Sociálnej poisťovne

V ..... dňa .....

Za dodávateľa:

.....
Ing. Martin Peluha
konateľ
DXC Technology Information
Services Slovakia s.r.o.

…….....
Zdenko Böhmer
konateľ
DXC Technology Information
Services Slovakia s.r.o.