Dohoda o spolupráci

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

(ďalej len „dohoda“)

uzatvorená medzi:

Názov organizácie:	**Finančné riaditeľstvo Slovenskej republiky**
Sídlo:	Lazovná 63, 974 01 Banská Bystrica
Štatutárny orgán:	Ing. Jiří Žežulka, prezident finančnej správy
IČO:	42 499 500

(ďalej ako „FR SR“)

Názov organizácie:	**SOFTIP, a. s.**
Sídlo:	Krasovského 14, 851 01 Bratislava – mestská časť Petržalka
Štatutárny orgán:	Ing. Dušan Guldan - predseda predstavenstva
IČO:	36 785 512

(ďalej ako „SOFTIP, a. s.“)

(ďalej spolu ako „strany dohody“)

Článok 1
Predmet dohody

1. Predmetom tejto dohody je dohoda uzatvorená medzi FR SR a SOFTIP, a. s. o tom, že SOFTIP, a. s. bude pre FR SR vykonávať služby a poradenstvo pri nasadzovaní a adopcii služieb Microsoft Windows E3, EMS E3 a Office 365 E1 za podmienok stanovených v tejto dohode.
2. Nasadzovaním a adopciou služieb uvedených v bode 1 tohto článku sa na účely tejto dohody rozumie:
   a) definícia M365 workloadov,
   b) výber vhodnej varianty hybridného riešenia,
   c) návrh integrácie na existujúce riešenia,
   d) vytvorenie Solution design (vrátane remediation a enablement),

e) výber a nasadenie riešenia identity,

f) vytvorenie networking topológie,

g) konfigurácia M365 služieb,

h) návrh a konfigurácia endpoint management a dvojfaktorovej autentifikácie,

i) návrh pravidiel pre prevádzku a podporu týchto služieb.

3. Táto dohoda je bezodplatná, prípadné náklady vzniknuté v súvislosti s plnením podľa tejto dohody si každá zo strán dohody platí sama.

Článok 2
Práva a povinnosti strán dohody

1. SOFTIP, a. s. sa touto dohodou zaväzuje:

a) vykonávať plnenia podľa tejto dohody s odbornou starostlivosťou, riadne a včas, a to za predpokladu potrebnej súčinnosti FR SR;

b) stretnutia a poskytovanie služieb vykonávať prednostne na diaľku, okrem prípadov, kedy to ich charakter nedovoľuje. Pri vykonávaní prác v sídle FR SR sa SOFTIP, a. s. zaväzuje dodržiavať predpisy o ochrane bezpečnosti práce a zdravia pri práci, požiarnej ochrany, hygieny práce a životného prostredia;

c) chrániť práva duševného vlastníctva FR SR a tretích osôb, ktoré by mohli byť plnením tejto dohody dotknuté;

d) dodržiavať podmienky, štandardy, nariadenia a opatrenia pri výkone na predmete dohody podľa článku 1 tejto dohody v súlade s aktuálne platnou legislatívou SR, primárne podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, 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, ako aj podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov, vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov a Všeobecné podmienky o zabezpečení informačnej bezpečnosti finančnej správy, ktoré tvoria Prílohu č. 1 tejto dohody pri prístupe k informačno-komunikačným technológiám finančnej správy (ďalej ako „IKT FS“);

e) pri spracúvaní osobných údajov spracúvaných v informačných systémoch FR SR postupovať v súlade s článkom 4 tejto dohody;

f) dodať predmet tejto dohody najneskôr do 8 mesiacov od účinnosti tejto dohody.

2. FR SR sa touto dohodou zaväzuje:

   a) s dostatočným predstihom poskytovať SOFTIP, a. s. potrebnú súčinnosť, úplné, pravdivé a včasné informácie potrebné pre riadne plnenie tejto dohody;

   b) umožniť SOFTIP, a. s. prístup k IKT FS za účelom plnenia tejto dohody.

3. Kontaktnou osobou za FR SR je [redacted], mobil: [redacted], e-mail: [redacted]

   Kontaktnou osobou za SOFTIP, a. s. je [redacted], mobil: [redacted], e-mail: [redacted]

Článok 3
Mlčanlivosť

1. Strany dohody sa dohodli, že všetky skutočnosti, informácie a údaje, o ktorých sa dozvedia v rámci spolupráce podľa tejto dohody, sa považujú za dôverné informácie, o ktorých sa obe strany dohody zaväzujú zachovávať mlčanlivosť, pokiaľ všeobecne záväzný právny predpis platný a účinný na území Slovenskej republiky alebo písomná dohoda strán dohody neustanovuje inak.

2. Za dôverné informácie sa nepovažujú skutočnosti, informácie a údaje, ktoré sú alebo sa stali verejne dostupnými, za podmienky že sa verejne dostupnými nestali porušením povinnosti mlčanlivosti podľa tejto dohody.

3. Povinnosť mlčanlivosti podľa tohto článku dohody trvá aj po zrušení alebo zániku tejto dohody.

4. Strany dohody sú povinné dôverné informácie utajovať a chrániť pred vyzradením, zneužitím, poškodením, zničením, stranou alebo odcudzením, a za týmto účelom sú povinné prijať primerané opatrenia.

5. Každá strana dohody je oprávnená poskytnúť dôverné informácie druhej strany dohody tretím osobám len s predchádzajúcim písomným súhlasom druhej strany dohody, a to len vo vzťahu k tretím osobám, ktoré majú participovať na vzájomnej spolupráci strán dohody vyplývajúcej z tejto dohody.

6. Strany dohody sú povinné obmedziť sprístupnenie dôverných informácií len tým zamestnancom strán dohody, ktorí budú participovať na spolupráci podľa tejto dohody a sú povinné zabezpečiť, aby sa povinnosť mlčanlivosti vyplývajúca z tohto článku dohody vzťahovala aj na tieto osoby. V prípade porušenia povinnosti zachovávať mlčanlivosť podľa tohto článku dohody zamestnancami strán dohody, zodpovedajú strany dohody za škodu spôsobenú ich zamestnancami.

7. Strany dohody sú oprávnené dôverné informácie použiť výlučne za účelom plnenia spolupráce podľa tejto dohody.

8. Neoprávnenú manipuláciu s dôvernými informáciami v rozpore s ustanoveniami tejto dohody je každá strana dohody povinná bezodkladne oznámiť druhej strane dohody.

9. Ak strana dohody poruší povinnosť podľa tohto článku dohody, je povinná zaplatiť druhej strane dohody pokutu vo výške 500 €, slovom: päťsto eur za každý jednotlivý prípad porušenia povinnosti zachovávať mlčanlivosť. Zaplatením pokuty podľa tohto bodu sa nevylučuje uplatnenie nároku na náhradu škody dotknutou stranou dohody. Povinnosť

[redacted]

strany dohody zaplatiť druhej strane dohody pokutu za porušenie povinnosti podľa tohto článku dohody vo výške stanovenej v tomto bode sa vzťahuje aj na prípady porušenia povinnosti zachovávať mlčanlivosť zamestnancami strán dohody podľa bodu 6 tohto článku dohody.

Článok 4
Ochrana osobných údajov

1. SOFTIP, a. s. bude osobné údaje, ktoré mu budú na základe plnenia predmetu tejto dohody zo strany FR SR počas trvania tejto dohody v rozsahu nutnom pre plnenie predmetu tejto dohody poskytnuté, resp. sprístupnené (ďalej len „predmetné osobné údaje"), spracúvať v súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov - ďalej len „Nariadenie GDPR") a so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 18/2018 Z. z.").
2. SOFTIP, a. s. je povinný zachovávať mlčanlivosť o predmetných osobných údajoch ako aj ich ochranu podľa Nariadenia GDPR a zákona č. 18/2018 Z. z., a to aj po skončení trvania tejto dohody, pričom o týchto povinnostiach je povinný preukázateľne poučiť aj všetkých zamestnancov, resp. oprávnené osoby SOFTIP, a. s., ktoré budú mať prístup k predmetným osobným údajom (ďalej len „predmetné osoby").
3. SOFTIP, a. s., ako aj všetky predmetné osoby, sú povinné spracúvať predmetné osobné údaje jedine na účel plnenia predmetu tejto dohody, pričom na iné účely predmetné osobné údaje nesmú spracúvať.
4. SOFTIP, a. s. je v súlade s Nariadením GDPR a so zákonom č. 18/2018 Z. z. povinný prijať také technické, personálne a organizačné opatrenia, ktoré zabezpečia primeranú ochranu predmetných osobných údajov a zabrániť hoci aj náhodnému zneužitiu, poškodeniu, zničeniu, strate, zmene alebo nedovolenému prístupu či sprístupneniu predmetných osobných údajov, ako aj akýmkoľvek iným neprípustným formám ich spracúvania.
5. SOFTIP, a. s. nesmie umožniť prístup k predmetným osobným údajom tretím osobám ani tretím stranám.
6. SOFTIP, a. s. nesmie spracúvať predmetné osobné údaje prostredníctvom sprostredkovateľa, t. j. prostredníctvom subjektu, ktorý by osobné údaje spracúval v mene SOFTIP, a. s. a na základe jeho pokynov.

Článok 5
Trvanie dohody

1. Táto dohoda sa uzatvára na dobu 12 mesiacov.
2. Dohodu je možné ukončiť:
    a) vzájomnou dohodou strán dohody,
    b) odstúpením,

c) výpoveďou.

3. V prípade vzájomnej dohody FR SR a SOFTIP, a. s. o ukončení tohto zmluvného vzťahu sa táto dohoda končí dňom uvedeným v písomnej dohode podpísanej štatutárnymi zástupcami strán dohody o skončení tejto dohody.
4. Každá zo strán dohody má právo od tejto dohody odstúpiť, a to s okamžitou platnosťou, pokiaľ druhá strana dohody podstatným spôsobom preukázateľne poruší ustanovenia tejto dohody alebo koná v rozpore s dobrými mravmi a napriek písomnému upozorneniu druhej strany dohody pokračuje v takomto konaní. Za podstatné porušenie tejto dohody sa považuje najmä porušenie ustanovení článku 3 tejto dohody.
5. Ktorákoľvek strana dohody môže túto dohodu vypovedať písomne a to aj bez uvedenia dôvodu v trojmesačnej výpovednej lehote, ktorá začína plynúť prvým dňom mesiaca nasledujúceho po jej doručení druhej strane dohody.
6. Písomné oznámenie o odstúpení od tejto dohody a písomná výpoveď sa doručujú druhej strane dohody vždy poštou na adresu uvedenú v záhlaví tejto dohody alebo osobne. Zásielka uložená na pošte sa považuje za doručenú po uplynutí troch pracovných dní odo dňa jej uloženia na pošte, aj keď sa adresát o tom nedozvie. Pri osobnom doručení zásielky má odmietnutie prevzatia zásielky za následok doručenie zásielky, a to momentom odmietnutia jej prevzatia.

Článok 6
Záverečné ustanovenia

1. Práva a povinnosti strán dohody vyplývajúce z tejto dohody a v tejto dohode bližšie neupravené sa riadia príslušnými ustanoveniami Obchodného zákonníka.
2. Akékoľvek zmeny a doplnenia tejto dohody je možné vykonať len formou písomných dodatkov, odsúhlasených oboma stranami dohody.
3. Táto dohoda nadobúda platnosť dňom jej podpisu oboma stranami dohody a účinnosť nadobudne dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky v súlade s § 47a ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
4. Táto dohoda sa vyhotovuje v štyroch (4) vyhotoveniach, pričom každá zo strán dohody obdrží dve (2) vyhotovenia.
5. Neoddeliteľnou súčasťou tejto dohody je jej príloha:

   Príloha č. 1 - Všeobecné podmienky o zabezpečení informačnej bezpečnosti finančnej správy
6. Strany dohody si túto dohodu prečítali a jej obsahu porozumeli. Vyhlasujú, že táto dohoda je prejavom ich slobodnej vôle, nie je uzatvorená v tiesni a ani za nápadne nevýhodných podmienok. Na znak súhlasu s jej obsahom túto dohodu vlastnoručne podpisujú.

Za FR SR:

v Bratislave dňa ...

Ing. Jiří Žežulka
prezident finančnej správy

Za SOFTIP, a. s.

v Bratislave dňa 19.1.2022

Ing. Dušan Guldan
predseda predstavenstva

VŠEOBECNÉ PODMIENKY O ZABEZPEČENÍ INFORMAČNEJ BEZPEČNOSTI FINANČNEJ SPRÁVY

I. Úvodné ustanovenia

Všeobecné podmienky pre zabezpečenie informačnej bezpečnosti finančnej správy stanovujú povinnosti externého subjektu (dodávateľa), ak predmet plnenia zmluvy uzatvorenej medzi dodávateľom a Finančným riaditeľstvom Slovenskej republiky (ďalej len „FR SR") alebo Ministerstvom financií Slovenskej republiky (ďalej len „MF SR"), ako objednávateľom (ďalej len „zmluva") súvisí s informačno-komunikačnými technológiami finančnej správy (ďalej len „IKT FS").

Na účely tohto dokumentu sa rozumie:

a) **aktívom** všetko, čo má pre finančnú správu (ďalej len „FS") hodnotu (fyzické komponenty, softvér, dáta, infraštruktúra, služby, ľudské zdroje, povesť, dobré meno finančnej správy...),

b) **APV** aplikačné programové vybavenie zväčša vo forme samostatnej aplikácie či programovej nadstavby,

c) **bezpečnostným incidentom** akýkoľvek spôsob narušenia bezpečnosti IKT FS, ako aj akékoľvek porušenie bezpečnostnej politiky a súvisiacich pravidiel,

d) **bezpečnosťou informačného systému** ochrana všetkých údajov, ktoré systém obsahuje a sú doň vkladané, spracúvané a prenášané, ako aj ochranu všetkých častí, teda technických, ale aj netechnických,

e) **informáciou** údaje, hodnoty, dáta spracúvané automatizovaným alebo neautomatizovaným spôsobom,

f) **neoprávneným prístupom** prístup, ktorý nebol schválený FS, nie je v súlade s ustanoveniami Bezpečnostnej politiky FS a IRA FS týkajúcich sa prístupu k IKT FS,

g) **citlivými informáciami** informácie, ktoré FS spracúva v zmysle všeobecne záväzných právnych predpisov a ochrana týchto informácií je vyžadovaná legislatívou. K citlivým informáciám patria: osobné údaje, daňové tajomstvo, bankové tajomstvo, obchodné tajomstvo, príp. poštové, telekomunikačné tajomstvo a informácie súvisiace s IKT FS,

h) **dostupnosťou** požiadavka, aby aktívum bolo na požiadavku oprávneného používateľa prístupné a schopné použitia,

i) **dôvernosťou** bezpečnostná požiadavka, ktorej naplnenie znamená, že informácia nie je dostupná alebo prístupná neautorizovaným jednotlivcom, entitám alebo procesom,

j) **externým subjektom** dodávateľ, t. j. fyzická osoba podnikateľ, právnická osoba a štatutárom právnickej osoby určené fyzické osoby, ktoré sú zamestnancami externého subjektu v zmysle pracovnoprávneho vzťahu, vrátane zamestnancov subdodávateľa, ktorí v zmysle uzatvoreného zmluvného vzťahu budú zabezpečovať plnenie predmetu zmluvného vzťahu v súvislosti s dodávaním alebo odoberaním tovarov, služieb alebo prác súvisiacich s IKT FS. Externý subjekt v plnej miere zodpovedá aj za činnosť zamestnancov subdodávateľa, ako by danú činnosť zabezpečoval externý subjekt,

k) **externým subjektom s osobitným postavením** kontrolný alebo iný oprávnený orgán Slovenskej republiky podľa všeobecného záväzného právneho predpisu (napr. NKÚ),

l) **subdodávateľom** poskytovateľ služieb a/alebo dodávateľ prác a/alebo tovaru, ktorý je v zmluvnom vzťahu s dodávateľom, a ktorý priamo plní zmluvné povinnosti a záväzky dodávateľa voči objednávateľovi,

m) **zamestnancom externého subjektu** zamestnanec, ktorý je v pracovnoprávnom vzťahu s externým subjektom, prostredníctvom ktorého bude externý subjekt zabezpečovať realizáciu požadovaných činností v zmysle zmluvného vzťahu. Na účely tejto smernice sa za zamestnanca externého subjektu považuje aj zamestnanec subdodávateľa len v tom prípade, že externý subjekt je v zmysle uzatvoreného zmluvného vzťahu oprávnený zadať svoju prácu subdodávateľom a to v celom rozsahu, alebo len čiastočne. Zoznam subdodávateľov musí byť súčasťou uzatvoreného zmluvného vzťahu externého subjektu. V prípade, že v čase uzatvorenia zmluvného vzťahu, ktorý ho oprávňuje vykonávať činnosti, ktoré súvisia s prístupom k IKT FS, nebol subdodávateľ známy a vstúpil do procesu v priebehu plnenia zmluvy, musí byť tento subdodávateľ odsúhlasený formou písomného dodatku k zmluvnému vzťahu, ktorý priamo plní zmluvné povinnosti a záväzky dodávateľa voči FS,

n) **prístupom externého subjektu k IKT FS** akýkoľvek prístup externého subjektu k hardvéru, softvéru alebo dátam IKT FS vrátane príslušnej dokumentácie k IKT FS v presne určenom nevyhnutnom rozsahu za predpokladu splnenia jedného bodu nasledovných podmienok tohto odseku, na základe ktorého je možné predložiť požiadavku pre prístup k IKT FS:

   1. externý subjekt je vo zmluvnom vzťahu s FS, ktorý súvisí s dodávaním alebo odoberaním tovarov, služieb alebo prác súvisiacich s IKT FS, ktorého súčasťou musia byť Všeobecné podmienky o zabezpečení informačnej bezpečnosti FS,
   2. externý subjekt má s MF SR podpísanú zmluvu o dodávaní alebo odoberaní tovarov, služieb alebo prác súvisiacich s IKT FS, ktorá zohľadňuje požiadavky FS pre zabezpečenie informačnej bezpečnosti FS, alebo má podpísanú dohodu o zabezpečení informačnej bezpečnosti s FR SR, ktorá vychádza zo Všeobecných podmienok o zabezpečení informačnej bezpečnosti FS,
   3. externý subjekt vykonáva činnosti na základe objednávky FR SR, ktorej nutnou súčasťou budú externým subjektom podpísané Všeobecné podmienky o zabezpečení informačnej bezpečnosti FS. Za uvedené zodpovedá zadávateľ pri vyhotovení objednávky.

o) **FS** finančná správa,

p) **IKT FS** súhrn nasledovných komponentov používaných na prípravu, spracúvanie, uchovávanie a distribúciu dát a na manažovanie informácií a procesov vo FS, okrem služieb prístupných širokej verejnosti z vonkajšieho prostredia, a to:

   1. servery, pracovné stanice, iné koncové zariadenia a príslušná dokumentácia,
   2. zariadenia diskových polí, SAN infraštruktúra, zálohovacie zariadenia a príslušná dokumentácia,
   3. sieťová infraštruktúra a sieťové komponenty (napr. smerovače, firewally) a príslušná dokumentácia,
   4. informačné systémy FS a ich aplikačné programové vybavenie a jeho vrstvy, ako napr. webová vrstva, aplikačná vrstva, databázová vrstva a príslušná dokumentácia,
   5. doplnkové aplikačné komponenty ako napr. scripty, batch súbory, aplikačné nadstavby,
   6. zariadenia pre hlasovú a audiovizuálnu komunikáciu implementované v sieťovej infraštruktúre FS (napr. pobočkové ústredne) a príslušná dokumentácia,
   7. Wi-fi komponenty,
   8. dáta a informácie spracúvané v informačných systémoch FS,
   9. písomné záznamy a ostatné informácie súvisiace s IKT FS.

q) **IP adresou** adresa zariadenia pripojeného do počítačovej siete, definovaná na základe Internet Protokolu,

r) **informačným aktívom** aktívum v prostredí IKT FS,

s) **informačnou bezpečnosťou** súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných aktív,

t) **informačným systémom** súhrn HW, operačného, aplikačného a ďalšieho SW, sieťovej infraštruktúry a jej prvkov, ktoré zabezpečujú zber, prenos, spracúvanie, uloženie, výber, distribúciu a prezentáciu informácií a dát,

u) **integritou** vlastnosť, že informácie a metódy ich spracúvania sú presné a kompletné,

v) **manažérom pre prístup k IKT FS** zamestnanec FS zodpovedný za posúdenie rozsahu požadovaného prístupu a oprávnení, oprávnenosť predloženej požiadavky, úplnosť vyplnenej žiadosti, eskaláciu realizácie prístupu k IKT FS a riešenie požiadaviek, ktoré súvisia s prístupom k IKT FS a sú preukázateľne zdokumentované FS. Oprávnenou osobou môže byť napr. PM, vlastník procesu, garant služby, riaditelia a vedúci útvarov sekcie informatiky (ďalej len „SI"), resp. písomne poverený iný zamestnanec FS určený SI na výkon úloh vyplývajúcich z činností spojených s externým prístupom k IKT FS,

w) **používateľom externého prístupu** zamestnanec externého subjektu, ktorému bol povolený externý prístup k IKT FS,

x) **MAC** adresou (**MAC - Media Access Control**) jedinečné identifikačné číslo sieťového adaptéra slúžiace na jednoznačnú identifikáciu daného sieťového rozhrania v LAN najmä typu Ethernet,

y) **VPN kanálom** vytvorené šifrované spojenie umožňujúce používateľom externého prístupu bezpečný prístup k požadovaným službám cieľovej infraštruktúry, resp. k IKT FS,

z) **zamestnancom FS**

1. príslušník FS v zmysle zákona č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. zamestnanec pri výkone práce vo verejnom záujme v zmysle zákona č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov,
3. zamestnanec vykonávajúci práce na základe dohôd o prácach vykonávaných mimo pracovného pomeru v zmysle zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov.

II. Základné požiadavky

1) Dodávateľ sa zaväzuje dodržiavať vnútorné predpisy objednávateľa, najmä Bezpečnostnú politiku FS, z ktorej vyplýva zabezpečenie informačnej bezpečnosti FS, ochranu všetkých aktív FS, ochranu informácií a IKT FS, prostredníctvom ktorých sa tieto informácie spracúvajú, prenášajú, ukladajú, bez ohľadu na formu v akej sa vyskytujú a spôsob ich spracúvania, vrátane podporných infraštruktúr týchto IKT FS.

2) Dodávateľ sa zaväzuje, že predmet plnenia zmluvného vzťahu a vykonávané činnosti budú v súlade s platnými požiadavkami legislatívy upravujúcej ochranu osobných údajov, daňového tajomstva, bankového tajomstva, obchodného tajomstva, príp. poštového, telekomunikačného tajomstva a iné.

3) Dodávateľ sa zaväzuje, že ak v rámci zmluvného vzťahu bude činnosť dodávateľa pozostávať okrem iného aj z činnosti, v rámci ktorej bude spracúvať osobné údaje[1], musia byť dodržané ustanovenia pre spracúvanie osobných údajov, vrátane práv, povinností a vzájomných vzťahov pri spracúvaní osobných údajov v zmysle Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „Nariadenie GDPR") a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 18/2018 Z. z.").

4) Dodávateľ sa zaväzuje dodržiavať ochranu osobných údajov, zachovávať mlčanlivosť o osobných údajoch, s ktorými počas výkonu prác príde do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu

[1] Článok 4 ods. 1 Nariadenia GDPR, resp. ustanovenie § 2 zákona č. 18/2018 Z. z.

osobných údajov Slovenskej republiky pri plnení jeho úloh, a to aj po ukončení zmluvného vzťahu, resp. ukončení pracovného pomeru zamestnancov dodávateľa.

5) Dodávateľ garantuje, že požadované činnosti v zmysle zmluvného vzťahu budú zabezpečované osobami s dostatočným bezpečnostným povedomím potrebným na výkon ich rolí a zodpovedností.

6) Dodávateľ garantuje, že zásahy do IKT FS bude realizovať výlučne iba v určenom rozsahu v rámci poskytnutých a dohodnutých prác a služieb v súlade so zmluvným vzťahom.

7) Dodávateľ sa zaväzuje, že v prípade, že by mal v úmysle zadať svoju prácu subdodávateľom, a to buď v celom rozsahu alebo len čiastočne, môže tak urobiť iba s predchádzajúcim písomným súhlasom objednávateľa a v takomto prípade zodpovedá, akoby zmluvu plnil sám. Zoznam subdodávateľov musí byť súčasťou predmetného uzatvoreného zmluvného vzťahu dodávateľa s objednávateľom. V prípade, že v čase uzatvorenia zmluvného vzťahu, ktorý ho oprávňuje vykonávať činnosti, ktoré súvisia s prístupom k IKT FS, nebol subdodávateľ známy a vstúpil do procesu v priebehu plnenia zmluvy, musí byť tento subdodávateľ odsúhlasený formou písomného dodatku k zmluvnému vzťahu, na základe ktorého plní zmluvné povinnosti a záväzky dodávateľa voči FS. Nedodržanie týchto povinností sa bude považovať za závažné porušenie zmluvných podmienok.

8) Dodávateľ sa zaväzuje, že prístup k IKT FS neposkytne a nebude žiadať pre iné osoby ako sú osoby, ktoré sú v pracovnoprávnom vzťahu s dodávateľom, resp. vo vzťahu so subdodávateľom, ktorý bol FS písomne schválený.

9) Dodávateľ garantuje, že požiadavku pre prístup k IKT FS, vrátane počtu osôb pre prístup k IKT FS a ich oprávnení, bude predkladať výlučne iba v rozsahu nevyhnutnom pre zabezpečenie plnenia úloh v zmysle predmetu plnenia zmluvy s cieľom poskytnutia služieb externého subjektu v prospech FS a je si vedomý, že všetky požiadavky prevyšujúce tento rozsah sú neprípustné a budú považované za porušenie zmluvných podmienok. Požiadavku pre prístup k IKT FS bude dodávateľ predkladať prostredníctvom žiadosti, ktorej vzor bude dodávateľovi poskytnutý FS a žiadosť bude podpísaná výlučne osobou, ktorá je oprávnená konať v mene dodávateľa.

10) Dodávateľ garantuje dodržiavanie bezpečnostných požiadaviek na ochranu aktív FS pred neautorizovaným prístupom, prezradením, modifikáciou, zničením alebo neoprávneným zásahom.

11) Dodávateľ garantuje zabezpečenie ochrany dôvernosti a integrity kódu a dokumentácie IS (do kontaktu s kódom a dokumentáciou informačného systému môžu prichádzať iba tí zamestnanci dodávateľa, ktorí podpísali Poučenie zamestnancov externého subjektu o informačnej bezpečnosti v prostredí IKT FS, ktoré tvorí prílohu č. 2 Smernice č. 17/2020.

12) Dodávateľ garantuje dodržiavanie požiadaviek na identifikáciu a autorizáciu zamestnancov externého subjektu pre prístup k IKT FS, zamestnanci sú povinní pristupovať k IKT FS výlučne s prideleným účtom pre dané prostredie FS, ktorý je spojený s jeho jednoznačnou identitou.

13) Dodávateľ garantuje, že pre prístup k IKT FS použije len FS schválený spôsob prístupu, resp. pripojenia k IKT FS.

14) Dodávateľ sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov (ďalej len „zamestnanec") realizujúcich úlohy, ktoré súvisia s plnením zmluvného vzťahu, dodržiavanie nasledovných povinností:

   a) zamestnanec je povinný zabezpečiť ochranu IKT FS a iných aktív FS pred ich poškodením, zničením, stratou, odcudzením, zneužitím, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím, ako aj pred akýmikoľvek inými neprípustnými spôsobmi ich použitia,

   b) zamestnanec je povinný dodržiavať ochranu citlivých informácií pred neoprávneným prístupom, zneužitím, poškodením, zničením, stratou, zmenou, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. K citlivým informáciám patria: osobné údaje, daňové tajomstvo,

bankové tajomstvo, obchodné tajomstvo, príp. poštové, telekomunikačné tajomstvo a informácie súvisiace s IKT FS,

c) zamestnanec je povinný zachovávať mlčanlivosť o citlivých informáciách, s ktorými počas výkonu činnosti príde do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenie, poskytnutie a sprístupnenie, a to aj po ukončení jeho pracovného, resp. zmluvného pomeru alebo po ukončení zmluvného vzťahu medzi dodávateľom a FS,

d) zamestnanec je povinný prístup k IKT FS vrátane pridelených technických prostriedkov FS používať výlučne len na plnenie pracovných úloh v zmysle zmluvného vzťahu s FS. Je prísne zakázané prístup k IKT FS vrátane iných aktív FS používať na iný účel, ako je plnenie pracovných úloh vyplývajúcich zo zmluvného vzťahu k FS,

e) zamestnanec, ktorý bude pristupovať k IKT FS, je povinný pripojenie, prístup a manipuláciu s IKT FS použiť len spôsobom, ktorý nie je v rozpore so všeobecne záväznými právnymi predpismi, bezpečnostnou politikou FS a internými predpismi FS, pričom pripojenie a prístup k IKT FS je zamestnanec povinný požívať iba v určenom rozsahu a s prístupovými právami, ktoré mu boli udelené v súlade s platnými pravidlami o prideľovaní prístupových práv vo FS a to výhradne na plnenie pracovných povinností v zmysle zmluvného vzťahu s cieľom poskytnutia služieb externého subjektu v prospech FS,

f) zamestnanec pristupuje a používa IKT FS výlučne s prideleným účtom pre dané prostredie FS, ktorý je spojený s jeho jednoznačnou identitou,

g) zamestnanec je povinný vyberať kvalitné heslá (tzn. heslá, ktoré nie sú citlivé na slovníkové útoky, nezadáva napr. dátum narodenia, po sebe identické znaky, atď.) a heslo musí spĺňať podmienky definované pre heslovú politiku k priradenému používateľskému účtu. Zamestnanec nesmie používať rovnaké heslá na pracovné a mimopracovné účely,

h) zamestnanec je povinný udržiavať prihlasovacie údaje/heslá v dôvernosti a zabezpečiť ochranu autentizačných údajov a predmetov pred zneužitím, odcudzením, prezradením inej osobe, tzn., že je prísne zakázané uchovávať heslá a autentizačné predmety na miestach dostupných iným osobám,

i) zamestnanec je povinný bezodkladne vykonať zmenu prihlasovacích údajov v každom prípade, keď existuje akákoľvek indícia kompromitácie týchto informácií a ohrozenia informačnej bezpečnosti FS,

j) zamestnanec môže na pracovných staniciach FS a iných technických prostriedkoch FS používať výlučne len programové vybavenie schválené a nainštalované FS - SI. Zamestnanec nemôže na pracovnej stanici FS meniť žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia,

k) zamestnancovi je prísne zakázané používať akýkoľvek program/aplikáciu slúžiacu na zachytávanie, resp. kompromitáciu hesiel,

l) zamestnanec je povinný dodržiavať opatrenia fyzickej a objektovej bezpečnosti tak, aby nedošlo k neoprávnenému prístupu k aktívam FS, k ich zneužitiu, odcudzeniu, poškodeniu ako aj dodržiavať požadovanú ochranu aktív pred možnými technickými poruchami a možnými prírodnými vplyvmi,

m) zamestnancovi je prísne zakázané vykonávať činnosť, ktorou by mohlo dôjsť k neautorizovanému prístupu k IKT FS, kompromitácii, alebo krádeži informácií a prostriedkov na ich spracúvanie,

n) zamestnancovi je prísne zakázané vykonávať činnosť, ktorou by neoprávnene zničil, poškodil, vymazal, pozmenil, alebo znížil kvalitu údajov v IKT FS,

o) zamestnancovi je prísne zakázané vykonávať činnosť, ktorou by neoprávnene vykonal zásah do technického alebo programového vybavenia IKT FS,

p) zamestnancovi je prísne zakázané vykonávať činnosť, ktorou by došlo k poškodeniu alebo zničeniu kľúčových komponentov IKT FS alebo k neočakávanému prerušeniu ich prevádzky,

q) zamestnancovi je prísne zakázané vykonávať činnosť, ktorou by neoprávnene vytváral neautentické dáta s úmyslom, aby sa dáta považovali za autentické,

r) zamestnancovi je prísne zakázané vykonávať činnosť za účelom získania prístupových práv alebo informácií IKT FS, ktoré mu neprináležia; ak takéto práva získa náhodne alebo vedome, nesmie ich použiť a musí o tom neodkladne a preukázateľne informovať FS - SI,

s) zamestnanec je povinný zabezpečiť primeraným mechanizmom ochranu všetkých aktív ponechaných bez dozoru, tzn. ukončenie, odhlásenie sa z IS/APV, blokovanie prístupu heslom, odhlásenie PC, zabezpečenie priestoru voči neoprávnenému vstupu do priestoru, kde sa aktíva FS nachádzajú, tak aby nedošlo k neoprávnenému prístupu k aktívam FS,

t) zamestnancovi je prísne zakázané prístup k IKT FS používať na realizáciu sieťových útokov, škodlivej činnosti namierenej proti používateľom alebo systémom FS,

u) zamestnanec je povinný vykonávať činnosť tak, aby nedošlo k šíreniu škodlivého kódu,

v) zamestnancovi je prísne zakázané vykonávať činnosti, ktorými by neoprávnene poskytol, sprístupnil, alebo zverejnil informácie/údaje FS,

w) zamestnanec nesmie pripájať technické zariadenia, ktoré nie sú v správe FS, bez súhlasu FS do siete FS,

x) zamestnanec je povinný pre externé pripojenie k IKT FS používať spôsob ochrany pripojenia formou VPN s autentizáciou certifikátom v kombinácii s menom a heslom, s privátnym kľúčom certifikátu uloženým na smart karte a chráneným PIN kódom. FS zamestnancovi zapožičia technické komponenty (čipovú kartu a čítačku čipovej karty) výlučne pre tento účel,

y) zamestnanec je povinný zabezpečiť ochranu autentizačných údajov a predmetov tak, aby nedošlo k ich odcudzeniu alebo zneužitiu,

z) zamestnanec je povinný neodkladne informovať FS o akejkoľvek nezhode medzi požadovaným a realizovaným prístupom k IKT FS,

aa) zamestnanec je povinný prístup k IKT FS z určených pracovných staníc z vyhradených pracovných priestorov FS realizovať v zmysle pokynov FS,

bb) zamestnanec je povinný neodkladne odovzdať FS zapožičané bezpečnostné predmety, vrátane všetkých poskytnutých zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty, čítačky čipových kariet a navrátenie informačných aktív (programy, dokumenty, údaje atď.), ktoré boli zamestnancovi externého subjektu (vrátane zamestnancov subdodávateľov) odovzdané a pominul dôvod, ktorý by ho oprávňoval ich disponovaním. Dôvodom vrátenia je:

1. ukončenie zmluvného vzťahu,
2. ukončenie doby platnosti schváleného prístupu k IKT FS,
3. ukončenie pracovnoprávneho vzťahu zamestnanca externého subjektu prípadne subdodávateľa,
4. iné skutočnosti, ktoré by ohrozili informačnú bezpečnosť FS, prípadne o ktorých bude dodávateľ informovaný FS.

15) Dodávateľ sa zaväzuje, že sa v žiadnom prípade bez vedomia objednávateľa nepokúsi získať prístup k informáciám, ktoré:

a) sú prenášané na sprístupnenej infraštruktúre FS,

b) nie sú pre neho potrebné na výkon požadovanej činnosti v zmysle zmluvného vzťahu a ani ich nezneužije v prípade, ak sa k nim neoprávnene dostane.

16) Dodávateľ sa zaväzuje zmeniť všetky prístupové hesla účtov, ktoré zostávajú naďalej aktívne, ak odchádzajúci zamestnanec dodávateľa poznal tieto heslá a to ihneď po ukončení pracovnoprávneho vzťahu vrátane vzťahu, ktorý sa týka zamestnancov subdodávateľa.

17) Dodávateľ sa zaväzuje, že o prístup k IKT FS požiada písomnou formou v súlade so Žiadosťou externého subjektu o prístup k IKT FS, ktorá tvorí prílohu č. 3 Smernice č. 17/2020 (ďalej len „Žiadosť") a ktorú mu FS poskytne vrátane požadovaných príloh, a to najneskôr jeden pracovný deň pred udelením prístupu k IKT FS.

18) Dodávateľ sa zaväzuje, že Žiadosť bude podpísaná osobou, ktorá je oprávnená konať v mene dodávateľa. Dodávateľ v súvislosti so zabezpečením plnenia úloh vyplývajúcich zo zmluvného vzťahu, ktoré súvisia s prístupom k IKT FS, môže písomne určiť osobu, ktorá bude oprávnená v mene dodávateľa konať. Dodávateľ doručí FR SR písomné splnomocnenie, ktorým určí túto oprávnenú osobu. V prípade akejkoľvek zmeny v súvislosti s touto oprávnenou osobou dodávateľ neodkladne písomne informuje FR SR.

19) Dodávateľ sa zaväzuje, že zabezpečí, aby všetky zásahy jeho zamestnancov do IKT FS boli zaznamenané v protokole z prístupu tretích strán k IKT FS. Zamestnanec dodávateľa po ukončení prác súvisiacich s prístupom vyplní tento protokol a ihneď ho e-mailom zašle oprávnenému zamestnancovi SI a následne mu ho podpísaný zašle aj v písomnej podobe a to do 5 pracovných dní od realizácie prístupu podľa prílohy, ktorú mu poskytne FS v zmysle požiadaviek interných predpisov FS upravujúcich riadenie prístupu externého subjektu k IKT FS.

20) Dodávateľ sa zaväzuje, že výstupy z IKT FS a všetky informácie získané pri prístupe k IKT FS budú slúžiť výlučne pre plnenie úloh vyplývajúcich zo zmluvného vzťahu k FS a je si vedomý, že je zakázané ich použiť na iný účel ako ten, na ktorý sú určené.

21) Dodávateľ sa zaväzuje a garantuje, že dodané dielo nebude obsahovať objednávateľom nevyžiadané alebo neschválené funkcie a vlastnosti, najmä nebude obsahovať funkcie a vlastnosti, ktoré by mohli viesť k zneužitiu, poškodeniu a kompromitácii IKT FS a nebudú vykonávané činnosti, ktoré nie sú požadované v zmysle zmluvného vzťahu.

22) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému, bude dielo odovzdané v súlade s technickou špecifikáciou požadovanou objednávateľom, ktorá nesmie byť v rozpore s požiadavkami zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 95/2019 Z. z."), v spojení s Vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov (ďalej len „Vyhláška ÚPVII") a v spojení s Výnosom Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov (ďalej len „Výnos MF SR"), a legislatívy upravujúcej ochranu informácií (ako sú osobné údaje, daňové tajomstvo, bankové tajomstvo, obchodné tajomstvo, príp. poštové, telekomunikačné tajomstvo a iné) a bude vykazovať funkčné vlastnosti ňou určené, ako aj ostatnými časťami zmluvného vzťahu.

23) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému, bude dielo odovzdané v súlade s platnými štandardmi pre informačné systémy verejnej správy v súlade s Výnosom MF SR účinným ku dňu riadneho prevzatia diela.

24) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému pre FS, bude najneskôr ku dňu riadneho prebratia diela odovzdaná nasledovná dokumentácia:

A. **Používateľská dokumentácia,** ktorá bude obsahovať minimálne popis na používanie IS:
   a. popis scenárov pre jednotlivé používateľské funkcie / role,
   b. popis všetkých bezpečnostných mechanizmov a procedúr vo vzťahu k používateľovi (popis správneho používania IS a popis zakázaného používania IS),
   c. popis chybových hlásení.

B. **Administrátorská dokumentácia obsahujúca popis na správu a prevádzku IS,** ktorá bude obsahovať minimálne:
   a. popis všetkých bezpečnostných mechanizmov a procedúr vo vzťahu k administrátorovi,
   b. popis funkcií pri administrácii,
   c. popis správy používateľov IS/APV,
   d. popis správy údajov v IS/APV,
   e. popis konfigurácie IS/APV,
   f. popis inštalácie klientskej aplikácie,

g. popis inštalácie a/alebo spôsob nasadenia nových verzií systému/APV, certifikátov,
h. popis a súpis predpísaných profylaktických činností,
i. popis všetkých používaných číselníkov,
j. popis a zoznam všetkých účtov
   i. systémových (popis použitia a ich umiestnenia),
   ii. aplikačných vrátane popisu ich rolí,
   iii. technologických.

C. **Prevádzková dokumentácia obsahujúca popis architektúry IS a jeho častí, jeho konfigurácií a väzieb na existujúce IS,** ktorá bude obsahovať minimálne:
   a. popis funkčnosti IS/APV (business model, funkčná špecifikácia...),
   b. popis detailnej architektúry IS/APV,
   c. popis databázovej štruktúry použitých databáz (význam polí v tabuľkách, prepojenia tabuliek, prepojenie DB serverov...),
   d. popis prevádzkových postupov a spôsob riešenia štandardných prevádzkových problémov,
   e. popis bezpečnostných procedúr a ovládanie bezpečnostných mechanizmov,
   f. popis funkcií pri prevádzke,
   g. popis konfigurácie IS a zapojenia,
   h. popis spôsobu zálohovania,
   i. popis spôsobu monitorovania prevádzky IS (z hľadiska záťaže, kapacít, konfigurácie, chýb),
   j. popis všetkých vzťahov a súvislostí nutných pre zabezpečenie plnej funkcionality dodaného diela a nadväzujúcich systémov a komponentov pri zmene hesiel aplikačných, systémových, inštalačných, ako aj technologických účtov prevádzkovateľom, vrátane bezpečného postupu popisujúceho detailne spôsob vykonania týchto zmien,
   k. popis detailného postupu pri obnove diela zo záloh,
   l. popis spôsobu a rozsahu monitorovania systémovej platformy,
   m. popis všetkých komunikačných rozhraní dodaného diela (obsahujúci informácie o type a účele rozhrania, procedúry, dátovej komunikácie, protokolov, a pod.).

D. **Posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov** v súlade s článkom 35 Nariadenia GDPR, resp. ustanovením § 42 zákona č. 18/2018 Z. z. v prípade, ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb.

25) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému FS, zabezpečí vyhodnotenie dodržiavanie požiadaviek zákona č. 95/2019 Z. z., Vyhlášky ÚPVII a Výnosu MF SR a to pred odovzdaním diela prostredníctvom preberacieho protokolu alebo akceptačného protokolu, ktorého súčasťou bude vyhlásenie o dodržiavaní štandardov pre informačné systémy verejnej správy formou podrobného rozpisu splnenia jednotlivých relevantných požiadaviek.

26) Dodávateľ sa zaväzuje, že súčasťou procesu odovzdania hotového diela je realizácia odborného zaškolenia určených zamestnancov FS zameraného na zvládnutie štandardných prevádzkových postupov a spôsobov riešenia bežných prevádzkových problémov.

27) Dodávateľ sa zaväzuje, že súčasťou procesu odovzdania hotového diela je poskytnutie komplexnej súčinnosti a podpory odborným zamestnancom FS pri zmene hesiel k aplikačným, systémovým, inštalačným a technologickým účtom.

28) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému FS, zabezpečí vykonanie bezpečnostných testov v týchto oblastiach, ktoré potvrdzujú, že dielo spĺňa funkčne bezpečnostné požiadavky:

a) testovanie potvrdzujúce súlad s dokumentáciou,

b) testovanie potvrdzujúce súlad s funkčnou špecifikáciou,
c) testovanie zraniteľnosti IS vrátane analýzy implementácie bezpečnostných funkcií,
d) aplikačné testy,
e) záťažové a výkonnostné testy,
f) „crash testy",
g) príp. iné doplňujúce bezpečnostné testy.

29) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému FS, po vykonaní bezpečnostných testov predloží FS správu o výsledku bezpečnostných testov s vyhlásením, že výsledky testov predkladá pravdivé a nepozmenené.

30) Dodávateľ zodpovedá za všetky priame alebo nepriame škody, ktoré svojím úmyselným alebo neúmyselným konaním spôsobí objednávateľovi a zaväzuje sa nahradiť ich objednávateľovi, vrátane sankcií za porušenie legislatívy.

III. Záverečné ustanovenia

31) Všeobecné podmienky o zabezpečení informačnej bezpečnosti FS sú záväzné pre dodávateľa v plnom rozsahu, pokiaľ v zmluve nie je ustanovené inak.

32) V prípade porušenia týchto všeobecných podmienok, v dôsledku ktorého vznikne škoda FR SR, sa dodávateľ zaväzuje nahradiť túto škodu.

33) Všeobecné podmienky o zabezpečení informačnej bezpečnosti FS sú súčasťou zmluvného vzťahu:

.....

V Bratislave dňa: [redacted]

Podpis: [redacted]

Ing. Dušan Guldan

Predseda predstavenstva SOFTIP, a. s.