[redacted]luva o vykonávaní auditu informačnej bezpečnosti

č. DC / 22 /2017

uzavretá v zmysle § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník
v znení neskorších predpisov medzi

1. **OBJEDNÁVATEĽ:**

Názov:	**Finančné riaditeľstvo Slovenskej republiky**
Zastúpený:	Ing. František Imrecze, prezident finančnej správy
Sídlo:	Lazovná 63, 974 01 Banská Bystrica
IČO:	42 499 500
DIČ:	2023395253

(ďalej len „objednávateľ")

2. **POSKYTOVATEĽ:**

Názov:	**DataCentrum**
Zastúpené:	Ing. Mojmírom Kollárom, riaditeľ DataCentra
Sídlo:	Cintorínska 5, 814 88 Bratislava
IČO:	00151564
DIČ:	2020845079

(ďalej len „poskytovateľ")

Čl. I.
Predmet zmluvy

1. Na základe tejto zmluvy sa poskytovateľ zaväzuje vykonávať audit informačnej bezpečnosti systémov DAC (DAC 1, DAC 2, DAC 4, (ďalej spolu len ako „systémy „DAC") objednávateľa podľa predloženého dotazníka vytvoreného na báze medzinárodnej normy ISO 27001 (ďalej len „výkon auditu"); vypracovať záverečnú správu z auditu v podobe vyplneného auditného dotazníka a potvrdiť certifikát podľa predloženého vzoru.
2. Systémy DAC zabezpečujú automatickú výmenu informácií medzi členskými štátmi EÚ v zmysle záväzkov SR vyplývajúcich zo smernice Rady 2011/16/EÚ z 15. februára 2011 o administratívnej spolupráci v oblasti daní a zrušení smernice 77/799/EHS, smernice Rady 2014/107/EÚ z 9. decembra 2014, ktorou sa mení smernica 2011/16/EÚ, pokiaľ ide o povinnú automatickú výmenu informácií v oblasti daní a smernice Rady (EÚ) 2016/881 z 25. mája 2016, ktorou sa mení smernica 2011/16/EÚ, pokiaľ ide o povinnú automatickú výmenu informácií v oblasti daní.
3. Objednávateľ vyhlasuje, že v zmysle Dohody o plnomocenstve a o výkone správcom určených činností, upravujúcich správu informačných systémov finančnej správy č. MF/035881/2013-295 uzavretej 22.5.2013 medzi Ministerstvom financií SR a Finančným riaditeľstvom SR a účinnej od 24.5.2013 je pre systémy DAC oprávnený uzatvoriť túto zmluvu.

4. Objednávateľ vyhlasuje, že uzatvára túto zmluvu za účelom splnenia povinností uloženým mu § 3 ods. 4 zákona č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZISVS"), a to najmä za účelom splnenia povinnosti:
   a. zabezpečenia bezpečnej prevádzky systémov DAC,
   b. zabezpečenia systémov DAC proti zneužitiu,
   c. zabezpečenia, aby boli systémy DAC v súlade so štandardmi informačných systémov verejnej správy, medzi ktoré patrí aj vykonávanie auditu informačnej bezpečnosti v súlade s § 32 písm. a) výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov.

Čl. II.
Termín a miesto plnenia

1. Miestom plnenia je sídlo objednávateľa: Lazovná 63, 974 01 Banská Bystrica.

2. Termín plnenia zmluvy začína plynúť dňom nadobudnutia jej účinnosti.

3. Zmluva sa uzatvára na dobu určitú s platnosťou 4 roky.

4. Termíny vykonania auditu informačnej bezpečnosti konkrétneho informačného systému DAC objednávateľa budú zmluvnými stranami dohodnuté prostredníctvom kontaktných osôb uvedených v čl. III. tejto zmluvy. Zmluvné strany týmto splnomocňujú kontaktné osoby uvedené v čl. III. tejto zmluvy na určenie termínov auditu informačnej bezpečnosti konkrétneho informačného systému DAC. Dohodnutý termínu vykonania auditu informačnej bezpečnosti konkrétneho informačného systému DAC objednávateľa zmluvné strany potvrdia písomným záznamom podpísaným oboma kontaktnými osobami.

5. Zmluvné strany sa dohodli pre prípad, že nedôjde počas trvania tejto zmluvy k dohode kontaktných osôb uvedených v čl. III. tejto zmluvy na určení termínu vykonania auditu informačnej bezpečnosti konkrétneho informačného systému DAC objednávateľa podľa príslušných ustanovení tejto zmluvy, dohodnú tento audit osoby oprávnené konať za zmluvné strany priamo formou dodatku k tejto zmluve. V prípade, že nedôjde k uzatvoreniu dodatku k tejto zmluve podľa predchádzajúcej vety, nepovažuje sa táto skutočnosť za porušenie povinnosti poskytovateľa podľa tejto zmluvy.

Čl. III.
Kontaktné osoby

1. Za objednávateľa bude kontaktnou osobou: [redacted]

2. Za poskytovateľa bude kontaktnou osobou: [redacted]

3. Zmluvné strany sú počas trvania tejto zmluvy oprávnené zmeniť určené kontaktné osoby podľa tohto článku zmluvy. V prípade, že ktorákoľvek zo zmluvných strán

bude mať počas trvania tejto zmluvy záujem na zmene určenia kontaktnej osoby, je povinná túto zmenu bez zbytočného odkladu písomne oznámiť druhej zmluvnej strane. Zmena v určení kontaktnej osoby je voči druhej zmluvnej strane účinná v deň nasledujúci po dni doručenia písomného oznámenia o určení kontaktnej osoby druhej zmluvnej strane.

Čl. IV.
Ochrana informácií

1. Zmluvné strany sú povinné zachovávať mlčanlivosť o skutočnostiach týkajúcich sa vykonania auditu, a to vrátane všetkých informácií týkajúcich sa postupov poskytovateľa spojených s výkonom auditu podľa tejto zmluvy. Ďalej sú zmluvné strany povinné zachovávať mlčanlivosť o akýchkoľvek informáciách označených druhou stranou ako dôverné, o ktorých sa dozvedeli pri uzatváraní tejto zmluvy alebo počas jej trvania pri výkone svojich práv a povinností z nej vyplývajúcich, najmä ich nesmú prezradiť tretej osobe, ani ich použiť v rozpore s účelom ich poskytnutia, pokiaľ táto zmluva neustanovuje inak.

2. Objednávateľ týmto poučuje poskytovateľa o skutočnosti, že informácie ktoré sa dozvie pri plnení tejto zmluvy, môžu byť predmetom daňového tajomstva. O tejto skutočnosti je poskytovateľ povinný poučiť aj svojich zamestnancov a osoby, ktoré budú v jeho mene plniť túto zmluvu.

3. Poskytovateľ sa zaväzuje dodržiavať Všeobecné podmienky o zabezpečení informačnej bezpečnosti finančnej správy (Príloha č. 1) v súvislosti s prístupom k informačno-komunikačným technológiám finančnej správy.

4. Poskytovateľ je oprávnený po ukončení výkonu auditu podľa tejto zmluvy vyhotoviť varovania, upozornenia, oznámenia, reakcie, analýzy (ďalej len „výstup"). Výstup nesmie obsahovať osobné údaje ani informácie, ktoré sú predmetom daňového tajomstva. Výstup je poskytovateľ oprávnený použiť pre internú potrebu a za podmienok stanovených touto zmluvou aj pre tretie osoby.

5. Poskytovateľ je povinný výstup, v prípade ak má byť použitý pre tretie osoby, tento anonymizovať do takej podoby, aby nebolo z výstupu zrejmé, že sa akékoľvek informácia obsiahnuté vo výstupe týkajú objednávateľa. Poskytovateľ je oprávnený výstup poskytnúť:
   a. iným subjektom, ktorí sú vlastníkom, správcom alebo prevádzkovateľom informačných systémov verejnej správy v zmysle príslušných ustanovení ZISVS,
   b. iným partnerom poskytovateľa v oblasti ochrany informačnej a komunikačnej infraštruktúry alebo kybernetickej bezpečnosti.

6. V prípade, že výstup vytvorený poskytovateľom by mal povahu autorského diela, je vykonávateľom všetkých práv duševného vlastníctva k tomto výstupu poskytovateľ.

Čl. V.
Odmena

1. Zmluvné strany sa dohodli, že poskytovateľ vykoná audit informačnej bezpečnosti systémov DAC pre objednávateľa bezodplatne.

Čl. VI.
Súčinnosť objednávateľa

1. Objednávateľ sa zaväzuje poskytnúť poskytovateľovi súčinnosť v rozsahu potrebnom na to, aby mohol poskytovateľ riadne uskutočniť výkon auditu podľa tejto zmluvy.
2. Poskytnutím súčinnosti zo strany objednávateľa zmluvné strany rozumejú najmä záväzok objednávateľa:
   a. umožniť poskytovateľovi prístup k systémom objednávateľa podliehajúcich výkonu auditu,
   b. zabezpečiť spoluprácu a kooperáciu zamestnancov a iných poverených osôb objednávateľa,
   c. umožniť poskytovateľovi prístup k akejkoľvek dokumentácii týkajúcej sa systémov objednávateľa podliehajúcich výkonu auditu.

Čl. VII.
Ukončenie zmluvy

1. Táto zmluva zaniká uplynutím času, na ktorý bola uzatvorená, dohodou zmluvných strán, uplynutím výpovednej doby a odstúpením od zmluvy.
2. Ktorákoľvek zo zmluvných strán môže písomne vypovedať túto zmluvu. Výpovedná lehota je 1 mesiac a začína plynúť dňom doručenia výpovede druhej zmluvnej strane.
3. Zmluvné strany sa dohodli, že odstúpiť od zmluvy možno z dôvodu porušenia akýchkoľvek ustanovení uvedených v tejto zmluve, pričom ak oprávnená zmluvná strana zamýšľa odstúpiť od zmluvy z dôvodov porušenia zmluvných povinností na strane druhej zmluvnej strany, je povinná písomne vyzvať druhú zmluvnú stranu na dodatočné splnenie povinností, ak to povaha povinností umožňuje, a poskytnúť k tomu dostatočnú lehotu na splnenie zmluvných povinností, minimálne sedem (7) dní. V prípade nesplnenia povinnosti ani v tejto dodatočnej lehote môže oprávnená zmluvná strana odstúpiť od zmluvy.

Čl. VIII.
Záverečné ustanovenia

1. Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch strán a účinnosť dňom nasledujúcim po dni jej prvého zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR.

2. Zmluvné strany vynaložia všetko úsilie na zmierne vyriešenie všetkých nezhôd alebo sporov vznikajúcich medzi nimi pri plnení zmluvy alebo v súvislosti s ňou, a to cestou priamych rokovaní.
3. Táto zmluva je vyhotovená v štyroch rovnopisoch, z ktorých dva rovnopisy obdrží objednávateľ a dva poskytovateľ.
4. Akékoľvek dodatky k tejto zmluve budú vypracované v písomnej forme v 4 rovnopisoch.
5. Zmluvné strany potvrdzujú, že túto zmluvu uzavreli slobodne, vážne, bez nátlaku, bez omylu, túto si pred jej podpisom prečítali, jej obsahu porozumeli a na znak súhlasu s jej obsahom ju podpísali.

V Banskej Bystrici,

Za objednávateľa [redacted]

Ing. František Imrecze

prezident finančnej správy

V Bratislave, [redacted]

Za poskytovateľa [redacted]

Ing. Mojmír Kollár

riaditeľ DataCentra

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 (ďalej len „FR SR") alebo Ministerstvom financií (ďalej len „MF") SR (ďalej len „zmluva") a 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 a 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** ochranu 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 spracovávané 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 finančná správa spracováva 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,

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

h) **externým subjektom** 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,

i) **externým subjektom s osobitným postavením** kontrolný alebo iný oprávnený orgán SR podľa všeobecného záväzného právneho predpisu (napr. NKU)

j) **subdodávateľom** sa rozumie 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,

k) **zamestnancom externého subjektu** zamestnanec, ktorý je v pracovnoprávnom vzťahu s externým subjektom, prostredníctvom ktorého bude externý subjekt zabezpečovať realizáciu požadovaných činnosti 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 (ďalej len „subdodávateľ") 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 neboľ 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,

l) **prístupom externého subjektu k IKT FS** akýkoľvek prístup externého subjektu k hardvéru alebo 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 IB s FR SR, ktorá vychádza zo Všeobecných podmienok o zabezpečení informačnej bezpečnosti FS.),
   3. externý subjekt, ktorý 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,

m) **FS** finančná správa,

n) **IKT FS** súhrn nasledovných komponentov používaných na prípravu, spracovanie, uchovávanie a distribúciu dát a na manažovanie informácií a procesov vo FS SR, 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, aplikačné 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 spracovávané v informačných systémoch FS,
   9. písomné záznamy a ostatné informácie súvisiace s IKT FS.

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

p) **Informačným aktívom** aktívum v prostredí IKT FS,

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

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

s) **integritou** vlastnosť, že informácie a metódy ich spracovania sú presné a kompletné,

t) **manažérom pre prístup k IKT FS** zamestnanec FS zodpovedný za posúdenie rozsahu požadovaného prístupu a oprávnení, oprávnenosť predloženej požiadavky, úplnosť vyplnenej žiadosti, eskalácie 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 resp. písomne poverený iný zamestnanec FS určený sekciou informatiky na výkon úloh vyplývajúcich z činností spojených s externým prístupom k IKT FS,

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

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

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

x) **zamestnancom FS**

1. zamestnanec vykonávajúci prácu vo verejnom záujme v zmysle zákona č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov,
2. zamestnanec v štátnozamestnaneckom pomere v zmysle zákona č. 400/2009 Z.z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 400/2009 Z. z."), a
3. colník, ktorý vykonáva štátnu službu podľa zákona č. 200/1998 Z. z. o štátnej službe colníkov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 200/1998 Z. z.").

II. Základne požiadavky

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

3) Dodávateľ sa zaväzuje, že ak zmluvný vzťah v zmysle ktorého bude činnosť dodávateľa pozostávať okrem iného aj z činnosti v rámci ktorej bude spracovávať osobné údaje[1], musia byť dodržané ustanovenia pre spracúvanie osobných údajov, vrátane práv, povinnosti a vzájomných vzťahov pri spracúvaní osobných údajov v zmysle § 8 zákona č. 122/2013 Z. z. zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

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 pre ochranu osobných údajov pri plnení jeho úloh, a to aj po ukončení zmluvného vzťahu, resp. ukončení pracovného pomeru zamestnancov.

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

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

[1] § 3 ods. 3 zákona č. 122/2013 Z.z. zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

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, ďalej len „poučenie").

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 pracovného, resp. zmluvného pomeru, zmluvného vzťahu s 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 so 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 prístupovými právami, ktoré mu boli udelené s platnými pravidlami o prideľovaní prístupových práv vo FS a to výhradne na plnenie pracovný povinnosti 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- sekciou informatiky. 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, 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- Sekciu informatiky,

s) zamestnanec je povinný zabezpečiť primeraným mechanizmom ochranu všetkých aktív ponechaných bez dozoru, tzn. ukončenie, odhlásenie sa zo IS/APV, blokovanie prístupu heslom, odhlásením 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) 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 s ich disponovaním. Dôvodom vrátenia je:
   a) ukončenia zmluvného vzťahu;
   b) ukončenia doby platnosti schváleného prístupu k IKT FS;
   c) ukončenie pracovnoprávneho vzťahu zamestnanca externého subjektu prípadne subdodávateľa;
   d) resp. iné skutočnosti, ktoré by ohrozili informačnú bezpečnosť FS, prípadne o ktorých bude dodávateľ informovaný FS.

14) 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.

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

16) Dodávateľ sa zaväzuje, že o prístup k IKT FS požiada písomnou formou v súlade so „Žiadosťou externého subjektu o prístup k IKT FS" podľa vzoru, ktorý mu FS poskytne vrátane požadovaných príloh najneskôr desať pracovných dní pred udelením prístupu k IKT FS.

17) 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.

18) Dodávateľ sa zaväzuje, že zabezpečí, aby všetky zásahy jej 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 FR SR 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.

19) 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.

20) 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.

21) 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. 275/2006 Z.z. o informačných systémoch verejnej správy v znení neskorších predpisova výnosu Ministerstva financií SR o štandardoch pre informačné systémy verejnej správy a legislatívou upravujúcou 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.

22) 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 Ministerstva financií SR o štandardoch pre informačné systémy verejnej správy účinným ku dňu riadneho prevzatia diela.

23) 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 administrácií,
   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
      - systémových (popis použitia a ich umiestnenia)
      - aplikačných vrátane popisu ich rolí,
      - technologických.

C. **Prevádzková dokumentácia obsahujúca popis architektúry IS a jeho časti, jeho konfigurácií a väzieb na existujúce IS,** ktorá bude obsahovať minimálne:
   a) popis funkčnosti IS/APV (bussines 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 účelu rozhrania, procedúry, dátová komunikácia, protokoly, a pod.),

D. **Bezpečnostný projekt** v súlade s požiadavkami zákona č.122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ak v zmysle zmluvného vzťahu dielo súvisí s vývojom a aktualizáciou informačného systému pre FS, v ktorom sa budú spracovávať osobné údaje.

24) Dodávateľ sa zaväzuje, že v zmysle zmluvného vzťahu, ktorý súvisí s vývojom a aktualizáciou informačného systému FS zabezpečí vyhodnotenie dodržiavanie požiadaviek zákona č. 275/2006 Z.z. a výnosu Ministerstva financií SR o štandardoch pre informačné systémy verejnej správy 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.

25) 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.

26) Dodávateľ sa zaväzuje, že súčasťou procesu odovzdania hotového diela je poskytnutie komplexnej súčinnosti a podpory odborným zamestnancom FS pri zmene hesiel k aplikačných, systémových, inštalačných a technologických účtov.
27) 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.

28) 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 nepozmenené.

29) 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.

[redacted]

III. Záverečné ustanovenia

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

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

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

Zmluva o vykonaní auditu informačnej bezpečnosti č. DC/22/2017

V Bratislave dňa [redacted]

[redacted]

štatutárny zástupca dodávateľa