Zmluva o poskytovaní služieb

uzavretá podľa § 261 ods. 2 v spojení s § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov
(ďalej len „zmluva")

Zmluvné strany

1.	**Objednávateľ:**	**Mesto Kežmarok**
	Sídlo:	Hlavné námestie č. 1, 060 01 Kežmarok
	Štatutárny zástupca:	**PhDr. Mgr. Ján Ferenčák, MBA, primátor mesta**
	IČO:	00326283
	DIČ:	2020697184
	IČ DPH:	Mesto Kežmarok nie je platcom DPH SK 2020697184 – zdaniteľná osoba registrovaná pre daň podľa § 7a zákona č. 222/2004 Z.z. o dani z pridanej hodnoty v znení neskorších predpisov
	Bankové spojenie:	UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky
	IBAN:	SK07 1111 0000 0066 0818 5127
	Telefón:	052/4660 101
	Fax:	052/4660 101
	e - mail:	primator@kezmarok.sk
	(ďalej len „**objednávateľ**“)	
2.	**Zhotoviteľ:**	**CORA GEO, s.r.o.**
	Sídlo:	A. Kmeťa 5397/23, 036 01 Martin
	Štatutárny zástupca:	Ing. Jozef Habiňák, konateľ spoločnosti
	IČO:	31612989
	DIČ:	2020433888
	IČ DPH:	SK2020433888
	Bankové spojenie:	Tatra banka, a.s. IBAN: SK67 1100 0000 0029 4808 5378
	Telefón:	052/2851411
	e – mail:	obchod@corageo.sk
	(ďalej len „**poskytovateľ**“)	

I. PREDMET PLNENIA

1. Predmetom tejto zmluvy je odplatné poskytovanie v tejto zmluve stanovených služieb/podpory poskytovateľom pre prevádzku a údržbu informačných systémov poskytovateľa, ktoré boli dodané objednávateľovi, a to informačného systému samosprávy (ďalej „CG ISS“), business intelligence systému (ďalej len „CG BI“),

dokumentačného informačného systému (ďalej len „CG DISS“), portálového informačného systému (ďalej len „CG WEB“), riešenia pre podporu elektronizácie úradu (ďalej len „CG eMesto“) spolu s integračným rozhraním v zmysle Dohody o integračnom zámere Mesta Kežmarok a NASES, a súvisiacich aktivít s cieľom zabezpečiť plnohodnotné využívanie dodaných produktov v nasledujúcich rokoch v nasledovnom členení:

- Údržba licencií dodaného licenčného softvéru
- Update – údržba licencií dodaného aplikačného softvéru
- Upgrade – technické zhodnotenie dodaného aplikačného softvéru
- Hot – line podpora
- Riadenie projektu
- Technická podpora
- Metodická podpora
- Školenia
- Bezpečnostná politika

(ďalej v texte len „podpora“) za podmienok uvedených v tejto zmluve vrátane jej príloh.

2. Výklad pojmov na účely tejto zmluvy:

ASW	- znamená aplikačný softvér,
LSW	- znamená licenčný softvér tretích strán,
ISS	- znamená informačný systém samosprávy,
NU	- znamená licencie pre pomenovaných používateľov,
ANU	- znamená licencia pre pomenovaného správcu,
Multi	- znamená licenciu pre neobmedzený počet používateľov,
APP	- znamemá licenciu, ktorá je poskytovaná pre už zakúpený počet používateľov NU alebo multi,
Portál Modul	- znamená licencia na Portál ISS,
CPU	- znamená hlavný procesor počítača,
ASFU	- znamená druh licencie,
HW	- znamená hardvérové vybavenie,
ČD	- znamená človeko dní = 8 človekohodín,
ČH	- znamená človekohodín = 60 minút práce jedného človeka,
HotLine	- znamená služba zhotoviteľa, komunikácia prostredníctvom mailov, telefonátov a vzdialenej správy,
SQL dávky	- znamená databázové dávky,
UPDATE	- znamená aktualizácia dodaného IS na novšiu verziu zo strany zhotoviteľa,
UPGRADE	- znamená dodanie vyššej verzie dodaného IS zo strany zhotoviteľa,
KZ	- kumulatívna zmena,
1 ČH	- znamená človekohodina = 60 min,
1 ČD	- znamená človekodeň = 8 ČH,
Ročná podpora	- znamená podpora poskytovaná v priebehu jedného kalendárneho roka,
FO	- znamená fyzická osoba,
PO	- znamená právnická osoba,
Autorský zákon	- znamená zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov,
Zmluvný rozsah	- znamená preplatený rozsah danej služby/ podpory na jeden rok,
HelpDesk	- znamená portál dodávateľa https://cghelpdesk.corageo.sk/ pre

zapisovanie požiadaviek objednávateľa.

3. Poskytovateľ týmto prehlasuje, že je v plnom rozsahu oprávnený vykonávať predmet tejto zmluvy.

4. Ročná podpora pozostáva z nižšie uvedených činností v bližšej špecifikácií uvedenej v prílohe č. 2 tejto zmluvy:

4.1 **LSW - Údržba licencií dodaného licenčného softvéru**

Aktualizácia verzií licenčného softvéru:

TYP	**Predmet / Názov**	**Rozsah**	**Jednotka pre výpočet update**
ORACLE	Database SE2 ASFU ročná podpora 1 CPU	1	ks

4.2 **UPDATE – Údržba licencií dodaného aplikačného softvéru**

- Priebežné vykonávanie zmien vyplývajúcich zo všeobecne platnej legislatívy, ktoré priamo súvisia s funkciami príslušného modulu aplikačného softvéru. Pre vylúčenie pochybnosti platí, že poskytovateľ je povinný vykonať priebežné legislatívne zmeny, ktoré priamo súvisia s funkciami príslušného modulu aplikačného softvéru (ďalej len „legislatívny update“) najneskôr do 90 kalendárnych dní potom, čo budú zo strany príslušného orgánu verejnej moci sprístupnené (zverejnené) všetky relevantné technické podmienky a požiadavky na vykonanie predmetného legislatívneho updatu (tzn. všetky relevantné vykonávacie predpisy, usmernenia, vyhlášky, nariadenia a/alebo iné dokumenty).
- Zaisťovanie kompatibility aplikačného softvéru s novými verziami operačného systému používaného objednávateľom.
- Zaisťovanie kompatibility integračného rozhrania voči Ústrednému portálu verejnej správy a centrálnym registrom FO,PO a adries.
- Oprava chýb aplikačného softvéru vo forme kumulatívnych zmien a nových verzií.
- Kontrola implementácie nových verzií softvéru a súvisiacich opráv Poplatok za používanie licencií v súlade s Autorským zákonom.
- Zapracovanie opisu zmien na dokumentácie k aplikačnému softvéru.
- Zoznam modulov aplikačného softvéru a počet licencií, ktorých sa týka UPDATE:

TYP	Podsystem	Predmet / Nazov	Rozsah	Jednotka
Modul	BI	CG BI		
Modul	BI	CG BI BASE - DN,EB,ER,EO,EF,ZM, DGR	0,5	APP
Modul	DISS	CG DISS		
Modul	DISS	CG_DISS	1	MULTI
Modul	WEB	CG eMesto BASE		
Modul	WEB	Document management system (DMS)	1	APP
Modul	DISS	Integračný modul eDesk	1	APP
Modul	WEB	FormFiller	1	APP
Modul	DISS	Integračný modul IAM	1	APP
Modul	DISS	Workflow manažment (WFM)	1	APP
Modul	DISS	Riadenie podaní	1	APP
Modul	WEB	CG eMesto EXT		
Modul	DISS	Listinný rovnopis	1	APP
Modul	DISS	Zaručená konverzia	1	APP

Modul	WEB	CRZ zverejňovanie	1	APP
Modul	WEB	UET,CUET zverejňovanie	1	APP
Modul	BASE	CG ISS BASE		
Modul	BASE	Dokumenty	1	MULTI
Modul	BASE	Domy a byty	1	MULTI
Modul	BASE	Elektronická komunikácia SMS, e-mail	1	MULTI
Modul	BASE	Kataster nehnuteľností	1	MULTI
Modul	BASE	Obyvatelia	1	MULTI
Modul	BASE	Podnikatelia a prevádzky	1	MULTI
Modul	BASE	Správa CG ISS	1	MULTI
Modul	BASE	Správa údajov	1	MULTI
Modul	BASE	Súpisné a orientačné čísla	1	MULTI
Modul	BASE	Voľby	1	MULTI
Modul	EKON	CG ISS EKONOMIKA		
Modul	EKON	Banka a Homebanking	1	MULTI
Modul	EKON	Exekúcie	1	MULTI
Modul	EKON	Fakturácia	1	MULTI
Modul	EKON	Majetok	1	MULTI
Modul	EKON	Miestne dane - Daň z nehnuteľností	1	MULTI
Modul	EKON	Miestne dane a poplatok za KO	1	MULTI
Modul	EKON	Objednávky	1	MULTI
Modul	EKON	Platobné poukazy	1	MULTI
Modul	EKON	Pokladňa	1	MULTI
Modul	EKON	Poštové poukážky	1	MULTI
Modul	EKON	Rozpočet a prístupové práva	1	MULTI
Modul	EKON	Sklad	1	MULTI
Modul	EKON	Účtovníctvo	1	MULTI
Modul	EKON	Zmluvy	1	MULTI
OPTION	EKON	BAR CODE - modul EP Pokladňa	1	APP
Modul	MZDY	CG ISS MZDY		
Modul	MZDY	Personalistika a mzdy	50	NU + 1ANU
Modul	EVID	CG ISS EVIDENCIE		
Modul	EVID	Stavebné činnosti	5	NU + 1ANU
Modul	ORG	CG ORG		
Modul	EKON	ORG_Ekonomika	50	NU + 1ANU
Modul	MZDY	ORG_Personalistika a mzdy	50	NU + 1ANU
Modul	DISS	ORG_Registratúra	50	NU + 1ANU
Modul	ISS	ORG_Správa prístupov	50	NU + 1ANU
Modul	INTEG	ORG Integračný modul na eDesk-na každú ORG	1	APP
Modul	WEB	CG WEB		
Modul	WEB	CG eGOV1 - Všeobecná zóna	1	APP
Modul	WEB	CG eGOV2 - Privátna zóna	1	APP
Modul	WEB	CG eGOV3 - eFORMs	1	APP
Modul	WEB	CG WEB Portál (Ročná podpora)	1	APP
Modul	WEB	GDPR - Evidencia výskytu a prístupu	1	APP

Modul	MsP_Park	CG MsP Park		
Modul	ISS	Parkovacie karty	5	NU + 1ANU
Modul	ISS	Mestská polícia	5	NU + 1ANU
Modul	WEB	MaMP	5	NU + 1ANU
OPTION	INTEG	Integrácia EVO - evidencia vozidiel	1	APP

4.3 **UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru**

- Technické zhodnotenie dodaného aplikačného softvéru (alebo zapracovanie špecifických požiadaviek).
- Špecifickou požiadavkou sa rozumie požiadavka, ktorá sa realizuje na podnet mesta a bude zabezpečovať spracovanie údajov objednávateľa podľa jeho postupov a návrhov, ktoré sú rozdielne od algoritmov dodávaných a zapracovaných do aplikačného softvéru, ktoré sa chápu ako štandardné.
- Špecifické analytické a programátorské práce, ktoré priamo nezasahujú do jednotlivých aplikácií, ale súvisia s prácou s nimi /napr. návrh a programovanie konverzného programu a pod./.
- Zapracovanie požiadavky sa uskutoční na základe dohody zmluvných strán, najneskôr do 5 mesiacov od potvrdenia požiadavky.
- **Zmluvný rozsah 50 ČH/rok**

4.3.1. UPGRADE individuálny - Špecifické analytické a programátorské práce

- Špecifické analytické a programátorské práce, ktoré priamo nezasahujú do jednotlivých aplikácií (CGBI, CG DISS, CG ISS, CG GISAM, CG eGOV), ale súvisia s prácou s nimi (napr. návrh a programovanie konverzného programu, rozšírenie licencií a pod.).
- Dopracovania aplikácií na základe požiadaviek podľa tohto bodu nebudú poskytovateľom ponúkané ostatným zákazníkom poskytovateľa bez súhlasu objednávateľa.
- Tento bod je pre aktuálny kalendárny rok voliteľný.

Rozsah 50 ČH/rok

4.4 **HotLine podpora**

- Telefonická podpora v pracovné dni minimálne v čase od 8:00 do 16:00 na tel. čísle 052/285 14 01
- Vzdialená správa.
- **Zmluvný rozsah: 60 ČH/rok**

4.5 **Riadenie projektu**

- Príprava a koordinácia
  - aktivít súvisiacich s plnením špecifických požiadaviek UPGRADE,
  - aktivít súvisiacich s integráciou ASW na okolité systémy,
  - metodických dní a školení pre objednávateľa.
- Sledovanie využívania HotLine – konzultácie k vykázaným činnostiam.
- Vypracovanie dokumentu „Správa o stave informačného systému za rok...“, v lehote do 30.6. nasledujúceho kalendárneho roka.
- **Zmluvný rozsah 32 ČH/rok**

4.6 **Technická podpora**

- Profylaktika.
- Databáza a dáta.
- Operačný systém a systémové prostriedky.
- Licenčný a aplikačný softvér.

- Hardvérové vybavenie a sieť.
- Udržiavanie testovacej databázy.
- **Zmluvný rozsah 16 ČH/rok**

4.7 **Metodická podpora**

- Osobné konzultácie pracovníka poskytovateľa so zamestnancami mesta za účelom riešenia konkrétnych otázok súvisiacich s využívaním informačného systému podľa článku I. ods. 1 tejto zmluvy.
- **Zmluvný rozsah 40 ČH/rok**

4.8 **Školenia/metodické dni**

- Odborné školenie modulov aplikačného softvéru.
- Účasť na odborných metodických dňoch.
- **Zmluvný rozsah 10 osôb/rok**

4.9 **Bezpečnostná politika**

- Aktualizácia dokumentu: Plán zálohy a obnovy produktov CG.
- **Zmluvný rozsah 1 x ročne**

II. MIESTO, ČAS A SPÔSOB PLNENIA

1. Miestom realizácie plnenia tejto zmluvy je sídlo a prevádzka poskytovateľa, miestom odovzdania predmetu zmluvy je sídlo objednávateľa, pokiaľ sa zmluvné strany nedohodli inak.
2. Zmluva sa uzatvára na dobu neurčitú. Servisné služby/podpora budú poskytované v rozsahu uvedenom v čl. I. ods. 4 tejto zmluvy.
3. Podpora podľa článku II. bude realizovaná nasledovne:

   3.1 Nové verzie LSW budú objednávateľovi dodané najskôr po ich vydaní autorskou spoločnosťou a po poskytovateľom overenej a potvrdenej kompatibilite s ASW v súlade s výrobným plánom poskytovateľa.

   3.2 Update ASW podľa ods. 2 tohto článku si bude objednávateľ preberať v elektronickej forme z internetovej stránky poskytovateľa na základe poskytnutého prístupového mena a hesla.

   3.3 Upgrade ASW za účelom zapracovania špecifických požiadaviek objednávateľa bude realizovaný v termíne a rozsahu podľa vzájomnej dohody zmluvných strán.

   3.4 Telefonickú podporu zabezpečí poskytovateľ minimálne v čase od 8:00 hod. do 16:00 hod. v pracovných dňoch na telefónnom čísle 052/285 14 01 V prípade, ak by poskytovateľ dočasne neposkytoval v určitých pracovných dňoch telefonickú podporu (napr. medzi vianočnými sviatkami a Novým rokom, školenie pracovníkov HotLine podpory) bude o tom objednávateľa v predstihu informovať.

   3.5 Riadenie projektu, technická podpora, metodická podpora a školenie budú realizované v termíne a v rozsahoch podľa vzájomnej dohody zmluvných strán.

   3.6 Odovzdanie a prevzatie realizovaných činnosti potvrdia obe zmluvné strany podpisom preberacieho protokolu (ďalej len „preberací protokol“).

   3.7 Poskytovateľ môže realizovať v ASW zmeny, ktoré zvyšujú úroveň a možnosti použitia ASW a zmeny v dôsledku vývoja operačných systémov, programovacích

prostriedkov, technológií a technických zariadení. Poskytovateľ bude o zmenách a požiadavkách z nich vyplývajúcich informovať objednávateľa.

3.8 Podpora nezrealizovaná v aktuálnom roku bude zrealizované v nasledujúcom období, teda objednávateľovi nezaniká právo na ich dodanie dňom ukončenia príslušného kalendárneho roku a poskytovateľovi povinnosť ich dodať, a to aj po skončení príslušného obdobia, avšak najneskôr do doby trvania tejto zmluvy.

3.9 Služby nad rámec predplatených rozsahov špecifikovaných v tejto zmluve sa budú realizovať na základe osobitnej objednávky alebo dodatkom k zmluve, pričom ich realizácia bude potvrdená preberacím protokolom podpísaným zástupcami vo veciach technických oboch zmluvných strán.

III. ZMLUVNÁ CENA PREDMETU DIELA

1. Cena za poskytovanie predmetu zmluvy bola určená na základe vykonaného verejného obstarávania, je v súlade so zákonom č. 18/1996 Z.z. o cenách v znení neskorších predpisov, vyhláškou MF SR č. 87/1996 Z.z., ktorou sa vykonáva zákon NR SR č. 18/1996 Z.z. o cenách v znení neskorších predpisov, je doložená rekapituláciou jednotlivej časti vyhotovenou poskytovateľom, ktorá tvorí prílohu č. 1 k tejto zmluve. Takto dohodnutá cena je pre poskytovateľa nemenná a záväzná a predstavuje čiastku vo výške:

2. Cena predmetu plnenia na kalendárny rok 2024 je nasledovná:

Predmet servisnej zmluvy	**Cena bez DPH**	**DPH (20%)**	**Cena s DPH**
LSW podľa čl. I. ods. 4.1	1 200,00 €	240,00 €	1 440,00 €
UPDATE podľa čl. I. ods. 4.2	29 667,00 €	5 933,40 €	35 600,40 €
UPGRADE podľa čl. I. ods. 4.3.	4 450,00 €	890,00 €	5 340,00 €
Služby podľa čl. I. ods. 4.4 - 4.9 v zmluvných rozsahoch	16 673,00 €	3 334,60 €	20 007,60 €
SPOLU (EUR)	**51 990,00** €	**10 398,00** €	**62 388,00** €

3. Objednávateľ pri určení predpokladanej hodnoty zákazky pri vykonaní verejného obstarávania postupoval v súlade s § 6 ods. 7 písm. a) zákona č. 343/2015 Z.z. o verejnom obstarávaní v znení neskorších predpisov a vychádzal z celkových skutočných nákladov na poskytnutie služby za predchádzajúcich 12 mesiacov upravených o predpokladanú priemernú **infláciu za obdobie rokov 2024 - 2027 vo výške 10%.**

4. Služby podľa článku I. v rozsahu špecifikovanom v Prílohe č. 1 budú realizované priebežne počas kalendárneho roka, za ktorý boli uhradené poplatky ročnej podpory, pričom konečný termín plnenia tejto zmluvy pre každý kalendárny rok je deň 31.12.

   4.1 Pre ďalšie kalendárne roky počas trvania tejto zmluvy bude na základe rozsahov činností uvedených v čl. I. v termíne do 25.1. nasledujúceho kalendárneho roku spracovaný poskytovateľom plánovaný aktuálny rozsah prác.

   4.2 Poskytovateľ pripraví rozsah plnenia na daný kalendárny rok podľa Prílohy č. 1 „Rekapitulácia ceny služieb za obdobie kalendárneho roka“, ktorý bude následne po písomnom odsúhlasení zástupcom objednávateľa vo veciach technických podľa ods. I.1 podkladom pre realizáciu služieb a fakturáciu v danom kalendárnom roku.

5. Ceny služieb pre nasledujúci kalendárny rok a ďalšie roky má právo poskytovateľ upraviť raz ročne (do 25.1.) a to o násobok koeficientu (miery) inflácie meranej indexom spotrebiteľských cien za predchádzajúci kalendárny rok, vyhlásený Štatistickým úradom Slovenskej republiky. Ceny produktov a služieb navýšené o koeficient (mieru) inflácie budú zaokrúhlené na dve desatinné miesta. Pre vylúčenie pochybností platí, že ak koeficient (miera) inflácie meranej indexom spotrebiteľských cien za predchádzajúci kalendárny rok, vyhlásený Štatistickým úradom Slovenskej republiky sa bude rovnať nule, alebo ak nadobudne zápornú hodnotu, tak sa ceny produktov a služieb dodávaných poskytovateľom nezmenia.

    5.1 V prípade, že budú zakúpené nové licencie ASW, LSW alebo bude do ASW doplnená funkčnosť alebo prepojenia na IS iných dodávateľov, ktoré zvýši náročnosť UPDATE, premietne sa výška jej ceny do základnej sumy pre výpočet UPDATE. Navýšenie UPDATE si zmluvné strany písomne odsúhlasia na úrovní zástupcov vo veciach technických.

    5.2 V prípade zmeny sadzby DPH bude k cene služieb pripočítaná DPH vo výške platnej ku dňu zdaniteľného plnenia.

6. Výška UPDATE pre aktuálny rok sa stanoví výpočtom z cenníkových cien jednotlivých modulov ASW, pričom pre moduly s počtom licencií viac ako 5NU (pomenovaný používateľ) + 1ANU (pomenovaný používateľ – správca) sa výška UPDATE vypočítava ako 19% z cenníkových cien jednotlivých modulov pre 50NU + 1ANU platných v danom kalendárnom roku.

IV. PLATOBNÉ PODMIENKY

1. Cena za predmet zmluvy bude poskytovateľovi uhradená na základe faktúr, ktoré poskytovateľ doručí objednávateľovi. Faktúry budú obsahovať náležitosti uvedené v zákone č. 222/2004 Z.z. o DPH v znení neskorších predpisov.
2. Platby za jednotlivé položky predmetu zmluvy budú realizované nasledovne:
    2.1 Faktúra za predmet zmluvy uvedený v čl. I. ods. 4.1 tejto zmluvy - údržba licencií dodaného licenčného softvéru v cene podľa čl. III. tejto zmluvy bude vystavená vždy v I. štvrťroku prebiehajúceho kalendárneho roka.
    2.2 Faktúra za predmet zmluvy uvedený v čl. I. ods. 4.2-4.9 tejto zmluvy v cene podľa čl. III. tejto zmluvy bude vystavená k 31.1., 30.4., 31.7. a 31.10. príslušného kalendárneho roka, a to vo výške výške ¼ ročnej ceny jednotlivých položiek.
3. Lehota splatnosti faktúr je 14 dní od jej doručenia objednávateľovi.
4. Objednávateľ má právo vrátiť nesprávnu alebo neúplnú faktúru do 10 dní od jej doručenia, pričom vrátenie má odkladný účinok na jej splatnosť a nová splatnosť začína plynúť nasledujúcim dňom po dni, kedy bola opravená faktúra doručená objednávateľovi. Dĺžka splatnosti týmto nie je dotknutá.
5. Podpisom tejto zmluvy objednávateľ v zmysle zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov zároveň udeľuje Poskytovateľovi súhlas na to, aby mu poskytovateľ vyúčtovával odmenu a iný nárok poskytovateľa Elektronickou faktúrou a poskytovateľ nadobúda oprávnenie vystavovať a zasielať objednávateľovi Elektronickú faktúru ako vyúčtovanie za plnenia poskytnuté objednávateľovi poskytovateľom na základe tejto zmluvy.

6. Doručovanie elektronickej faktúry

7. Poskytovateľ sa zaväzuje doručovať Elektronickú faktúru objednávateľovi formou elektronickej pošty, a to na emailovú adresu Objednávateľa podatelna@kezmarok.sk (ďalej len „emailová adresa“) ako dokument PDF (s príponou *.pdf). Prílohy k faktúram a oznamy môžu byť vystavené vo formáte súborov pdf, doc, docx, xls, xlsx, tif alebo jpg. Na zabezpečenie vierohodnosti a neporušenosti údajov elektronických dokumentov nie je oprávnená žiadna zmluvná strana zasahovať ani meniť obsah už odoslaných dokumentov.

   7.1 Objednávateľ vyhlasuje, že má prístup k e-mailovej adrese, a že si je vedomý skutočnosti, že údaje sprístupnené mu v Elektronickej faktúre doručenej mu na e-mailovú adresu sú dôverné informácie, ktoré je každá zmluvná strana povinná utajovať, okrem prípadov, ak je ich sprístupnenie tretej osobe vyžadované platnými právnymi predpismi.

   7.2 Elektronická faktúra sa považuje za doručenú v deň nasledujúci po dni jej preukázateľného odoslania objednávateľovi poskytovateľom prostredníctvom elektronickej pošty na e-mailovú adresu.

V. REALIZÁCIA – PODMIENKY VYKONANIA DIELA

1. Na splnenie predmetu plnenia v čase plnenia je nutná spolupráca objednávateľa s poskytovateľom. V prípade, že objednávateľ neposkytne primeranú súčinnosť poskytovateľovi, poskytovateľ nie je v omeškaní s plnením tejto zmluvy a nenesie zodpovednosť za prípadne škody ktoré môžu v tejto súvislosti vzniknúť. Za účelom predchádzaniu daným skutočnostiam, zmluvné stany stanovili podmienky pre vzájomnú spoluprácu:

   1.1 objednávateľ určí zodpovednú a kompetentnú osobu pre styk s poskytovateľom počas plnenia predmetu zmluvy u objednávateľa do 5 pracovných dní od podpisu tejto zmluvy,

   1.2 objednávateľ zabezpečí požadovanú informačnú a organizačnú podporu a súčinnosť do 3 pracovných dní od vzniku požiadavky poskytovateľa vrátane požadovaného technického vybavenia, ak sa zmluvné strany nedohodli inak,

   1.3 objednávateľ určí zoznam kompetentných pracovníkov – odborných garantov objednávateľa do 5 pracovných dní od podpísania tejto zmluvy. Tento zoznam sa môže operatívne meniť a dopĺňať podľa potrieb a personálnych zmien u objednávateľa,

   1.4 za objednávateľa sú osoby podľa bodu 1.3 tohto odseku oprávnené požadovať realizáciu HotLine podpory a sú súčasne zodpovedné za čistotu a správnosť dát týkajúcich sa príslušných modulov, pre ktoré boli stanovení ako odborní garanti,

   1.5 za poskytovateľa sú tieto osoby zodpovedné za funkčnosť príslušných modulov, pre ktoré boli stanovení ako odborní garanti,

   1.6 zoznam zodpovedných osôb za obe zmluvné strany bude vedený písomne. Každá ďalšia zmena zodpovedných osôb – odborných garantov sa oznámi druhej zmluvnej strane vo forme listu, ktorý bude zaslaný do 10 pracovných dní odo dňa vykonania zmeny a podpísaný oprávnenou osobou,

1.7 objednávateľ je povinný zabezpečiť minimálne technické podmienky v zmysle špecifikácie podľa prílohy 3 tejto zmluvy a udržať ich (samozrejme môže aj prevýšiť) počas platnosti tejto zmluvy,

1.8 poskytovateľ je povinný oznámiť objednávateľovi prípadnú zmenu minimálnej technickej špecifikácie pre nasledujúce obdobie dostatočne včas, minimálne 6 mesiacov pred požadovaným termínom jej implementácie to neplatí v prípade realizácie legislatívneho update upraveného v článku I. ods. 4.2, prvá odrážka tejto zmluvy.

2. Za poskytovateľa sú za vykonanie predmetu plnenia zodpovední nasledovní pracovníci:

2.1 za koordináciu činností a realizáciu tejto zmluvy: Ing. Radka Kačmareková

2.2 za sledovanie čerpania hotline podpory: Ing. Radka Kačmareková

2.3 za realizáciu technickej podpory: 24 TP

3. Poskytovateľ bude bez meškania písomne informovať objednávateľa o vzniku akejkoľvek udalosti, ktorá bráni alebo sťažuje realizáciu predmetu tejto zmluvy.

4. Pri plnení predmetu plnenia sa obe zmluvné strany zaväzujú dodržiavať zásady informačnej bezpečnosti.

4.1 V prípade, ak pri poskytovaní podpory zo strany Poskytovateľa v súlade s prílohou č. 2 alebo pri poskytovaní iných služieb, na ktorých dodanie sa Poskytovateľ v súlade s touto Zmluvou zaviazal bude nevyhnutné, aby Poskytovateľ spracovával v mene Objednávateľa ako prevádzkovateľa osobných údajov osobné údaje fyzických osôb, zaväzuje sa Objednávateľ o tejto skutočnosti s dostatočným časovým predstihom Poskytovateľa informovať a súčasne sa zmluvné strany zaväzujú ešte pred tým ako dôjde k spracovaniu osobných údajov zo strany Poskytovateľa ako sprostredkovateľa osobných údajov uzatvoriť zmluvu o spracovaní osobných údajov a to v súlade s čl. 28 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“ alebo “GDPR“. Zmluvné strany sú následne povinné zabezpečiť splnenie všetkých povinností, ktoré citované Nariadenie pre spracovanie týchto osobných údajov dotknutých osôb Objednávateľa zo strany Poskytovateľa ako sprostredkovateľa vyžaduje a bez splnenia týchto osobitných podmienok stanovených Nariadením nie je Poskytovateľ oprávnený a ani povinný takéto osobné údaje Objednávateľa spracovávať.

5. Pre zabezpečenie ochrany údajov objednávateľa sa zmluvné strany dohodli, že:

5.1 prevzatie a následné odovzdanie akýchkoľvek dát resp. podkladov objednávateľa zo strany poskytovateľa bude realizované po udelení súhlasu písomnou alebo emailovou formou,

5.2 poskytovateľ je oprávnený dáta objednávateľa získané počas realizácie predmetu plnenia používať výlučne v súlade s účelom za ktorým boli poskytnuté,

5.3 poskytovateľ nemôže poskytnúť dáta objednávateľa alebo ich časť žiadnej tretej osobe ani publikovať dáta alebo jej časť akýmkoľvek verejne dostupným spôsobom bez písomného súhlasu objednávateľa,

5.4 poskytovateľ musí vynaložiť primerané úsilie na zabezpečenie dát objednávateľa pred stratou, znehodnotením alebo poškodením,

5.5 Zmluvné strany sa dohodli, že osobné údaje môže poskytovateľ spracovávať aj prostredníctvom subdodávateľa, ktorý ich bude spracovávať a zabezpečovať ich ochranu na zodpovednosť poskytovateľa.

6. Pre realizáciu vzdialeného prístupu poskytovateľa k informačným systémom objednávateľa sa zmluvné strany dohodli, že:

6.1 zamestnanci poskytovateľa v spolupráci s objednávateľom zabezpečia všetky potrebné technické náležitosti tak, aby bolo možné bezpečne využívať službu vzdialenej správy u objednávateľa, ako na samotnú technickú podporu, tak i pre potreby realizácie predmetu plnenia,

6.2 poskytovateľ zabezpečí internú evidenciu parametrov pripojenia pre vzdialenú správu v samostatnom súbore s riadeným prístupom výhradne pre pracovníkov, ktorí toto pripojenie realizujú,

6.3 poskytovateľ zabezpečí internú evidenciu účtov pre vzdialenú správu v samostatnom súbore prístupnom výhradne pre administrátorov pripojenia a account manažéra poskytovateľa,

6.4 na realizáciu vzdialenej správy sa v zásade vytvára jeden účet s privilégiami administrátor, ktorý je pridelený oddeleniu technickej podpory poskytovateľa a za jeho používanie a evidenciu použitia je zodpovedný poskytovateľ,

6.5 pre potreby projektu je možné vytvoriť ďalšie účty (bez administrátorských privilégií) na požiadanie account manažéra poskytovateľa na základe súhlasu povereného zamestnanca objednávateľa,

6.6 počas práce na zariadeniach objednávateľa prostredníctvom vzdialenej správy sa poskytovateľ zaväzuje dodržiavať všetky zásady ochrany údajov a zariadení objednávateľa; pre potreby spätného dohľadania a monitorovania činností, zabezpečí poskytovateľ vytvorenie záznamov (log súborov) o použití vzdialenej správy,

6.7 zamestnanec poskytovateľa realizujúci podporu (akoukoľvek formou) u objednávateľa je povinný najmä zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku pri prácach na informačných systémoch objednávateľa; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa informačného systému a zamestnávateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť,

6.8 poskytovateľ zabezpečí formou interného predpisu povinnosť mlčanlivosti jeho zamestnancov, ktorá bude trvať aj po zániku prístupu k podpore objednávateľa alebo po zmene pozície či ukončení pracovného pomeru,

6.9 povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov, pri plnení jeho úloh.

7. Zmluvné strany si dohodli nasledujúce postupy pri aktualizácii existujúcich riešení v prostredí informačných systémov (ďalej IS) objednávateľa vrátane riešenia požiadaviek a chýb:

7.1 všetky aktualizácie ASW vo forme verzií a kumulatívnych zmien (ďalej KZ) budú realizované sprístupnením príslušných aktualizačných súborov; samotnú aktualizáciu vykoná správca IS objednávateľa alebo osoba ním poverená,

7.2 zmeny v databáze ASW budú vykonávané zaslaním SQL dávky, ktorá tieto zmeny realizuje; spustenie dávky bude realizovať správca IS alebo osoba ním poverená,

7.3 v mimoriadnych prípadoch je možné po vzájomnej dohode určiť pre ods. 7.1 a 7.2 tohto článku zmluvy iný postup; tento postup musí byť presne definovaný a obmedzený na daný mimoriadny prípad,

7.4 pre účely tejto zmluvy – ods. 7.3 tohto článku zmluvy sa mimoriadnym prípadom rozumie stav, keď objednávateľ nie je schopný zabezpečiť aktualizáciu ASW a hrozí jeho nedostupnosť alebo nesprávna funkčnosť.

8. Žiadna zo zmluvných strán nesmie sprístupniť tretej osobe, alebo pre seba či iného využiť dôverné informácie, ktoré pri plnení tejto zmluvy získala od druhej zmluvnej strany. Zmluvné strany môžu sprístupniť dôverné informácie za účelom plnenia tejto zmluvy zamestnancom podieľajúcim sa na plnení podľa tejto zmluvy za rovnakých podmienok, aké sú stanovené zmluvným stranám v tomto článku, a to len v rozsahu nevyhnutnom pre riadne plnenie tejto zmluvy. Ďalej ich môžu sprístupniť tretím osobám za účelom uskutočnenia právneho, účtovného alebo daňového auditu niektorej zo zmluvných strán, ak sú tieto osoby viazané povinnosťou ochrany informácií najmenej v rozsahu, aký je stanovený v tomto článku. Dôverné informácie sú považované zmluvnými stranami za obchodné tajomstvo a obidve zmluvné strany sa ho zaväzujú takto chrániť.

   8.1 Za dôverné informácie sú na základe tejto zmluvy stranami považované všetky informácie vzájomne poskytnuté v ústnej alebo v písomnej forme, najmä informácie, ktoré sa strany dozvedeli v súvislosti s touto zmluvou, ako aj know-how, ktorým sa rozumejú všetky poznatky obchodnej, výrobnej, technickej či ekonomickej povahy súvisiace s činnosťou zmluvnej strany, ktoré majú skutočnú alebo aspoň potenciálnu hodnotu, a ktoré nie sú v príslušných obchodných kruhoch bežne dostupné a majú byť utajené.

   8.2 Zmluvné strany sa zaväzujú zachovávať mlčanlivosť o informáciách, o ktorých sa dozvedeli pri realizácii predmetu zmluvy. Žiadne informácie spojené s predmetom zmluvy a zvlášť tie, ktoré sú bližšie špecifikované v prílohe č.1, 2, 3 nesmú byť použité na iné účely ako je definované v tejto zmluve a nesmú byť poskytnuté tretej osobe a to ani po skončení právneho vzťahu založeného touto zmluvou. Zmluvné strany sú si zároveň vedomé právnych následkov porušenia tejto povinnosti.

9. Zmluvné strany budú mať pri plnení tejto zmluvy prístup k informáciám týkajúcim sa druhej zmluvnej strany (ďalej len „dotknutá zmluvná strana“) a jej podnikania, najmä k akýmkoľvek informáciám obchodnej, výrobnej, prevádzkovej, marketingovej, finančnej, majetkovej, organizačnej, personálnej, hospodárskej a/alebo technickej povahy, vrátane analýzy a opisu činnosti modulov. Tieto informácie alebo akékoľvek iné informácie verejne neprístupné a súvisiace s činnosťou dotknutej zmluvnej strany, ktoré druhá zmluvná strana získa ústne, písomne alebo v akejkoľvek inej forme pri plnení tejto zmluvy alebo v jej súvislosti, sú predmetom obchodného tajomstva dotknutej zmluvnej strany, alebo ich dotknutá zmluvná strana týmto označuje ako dôverné v zmysle ustanovenia § 271 Obchodného zákonníka (ďalej len „dôverné informácie“).

10. Zmluvné strany budú zachovávať mlčanlivosť o dôverných informáciách, najmä sa zaväzujú s dôvernými informáciami zaobchádzať ako s prísne tajnými, tieto dôverné informácie bez výslovného predchádzajúceho písomného súhlasu dotknutej zmluvnej strany priamo alebo nepriamo tretej osobe neoznámiť, nesprístupniť, nezverejniť alebo pre seba alebo iného nevyužiť.

11. Zmluvné strany písomne oznámia dotknutej zmluvnej strane akékoľvek okolnosti, ktoré by mohli viesť k vzniku konfliktu záujmov s dotknutou zmluvou stranou.

12. Zmluvné strany použijú dôverné informácie iba v súvislosti s plnením predmetu tejto zmluvy a na dosiahnutie účelu podľa tejto zmluvy.
13. Zmluvné strany obmedzia zverenie dôverných informácií iba tým svojim zamestnancom, ktorí sú určení na plnenie predmetu tejto zmluvy, a u ktorých zabezpečujú dodržiavanie dôvernosti týchto informácií a povinností s tým súvisiacich.
14. Zmluvné strany o každom sprístupnení dôverných informácií tretej strane v prípadoch stanovených všeobecne záväznými právnymi predpismi budú informovať dotknutú zmluvnú stranu.

VI. ZODPOVEDNOSŤ ZA CHYBY, ZÁRUKY

1. V súvislosti s chybami ASW je určená nasledovná kategorizácia chýb ASW:
   1.1 **Kritická chyba** – chyba, ktorá má vplyv na podstatné činnosti ASW, pričom ASW nie je možné u objednávateľa používať na zabezpečenie činností opísaných v prílohách k jednotlivým zmluvám o dielo, týkajúcich sa objednávateľom zakúpených modulov a objednávateľ nemôže použiť iné moduly ASW na realizáciu činností.
   1.2 **Hlavná chyba** – chyba, ktorá neumožňuje prácu s ASW podľa opisu v dokumentácii bez použitia iných metodických a technologických postupov.
   1.3 **Malá chyba** – chyba, ktorá nemá vplyv na spoľahlivosť a spôsob používania ASW v plynulej prevádzke.
2. Reklamácia chyby predmetu zmluvy bude uplatnená písomne.
   2.1 Objednávateľ sa zaväzuje, že prípadnú reklamáciu chyby dodaného ASW uplatní bezodkladne po jej zistení formou helpdesk alebo email. Každá reklamácia bude zaslaná aj v písomnej forme listom na adresu sídla poskytovateľa, inak na reklamáciu poskytovateľ neprihliada.
   2.2 V reklamácií objednávateľ čo najpresnejšie opíše charakter reklamovanej chyby a zaradí chybu do kategórie chýb podľa ods. 1 tohto článku zmluvy. Potvrdenie prijatia reklamácie zo strany poskytovateľa bude realizované podľa spôsobu jej ohlásenia.
   2.3 Poskytovateľ je povinný reagovať - potvrdiť prijatie - na každú reklamáciu do 18 hodín od jej doručenia (helpdesk, email) pričom do reakčnej doby je zahrnutá iba pracovná doba od 8:00 do 16:00 hod. a počas pracovných dní. V prípade doručenia reklamácie na konci pracovného času/ pracovnej doby sa čas reakcie na reklamáciu počíta v príslušnom zostatku do pracovného času nasledujúceho pracovného dňa.
3. Poskytovateľ sa zaväzuje začať činnosti potrebné na odstránenie chyby do 24 hodín od potvrdenia jej prijatia (reakčná doba) pričom do reakčnej doby je zahrnutá iba pracovná doba od 8:00 do 16:00 hod. počas pracovných dní. Pričom prvotne zaradí reklamáciu/ chybu do kategórie chýb a dané oznámi objednávateľovi spolu s časom na jej odstránenie. Čas na odstránenie chyby začína plynúť od potvrdenia reklamácie u poskytovateľa a zaradenia chyby do kategórie chýb v zmysle ods. 1 tohto článku zmluvy.
4. Poskytovateľ sa zaväzuje odstrániť chyby nasledovne, ak sa strany nedohodnú inak:
   4.1 kritickú chybu podľa ods. 1.1 tohto článku do 2 pracovných dní od uplynutia reakčnej doby, ak sa strany nedohodnú inak,

4.2 hlavnú chybu podľa ods. 1.2 tohto článku do 30 dní pracovných dní od uplynutia reakčnej doby, ak sa strany nedohodnú inak,

4.3 malú chybu podľa ods. 1.3 tohto článku v rámci najbližšej plánovanej verzie ASW.

5. Za odstránenie chyby sa považuje aj jej preradenie do novej kategórie chýb na základe čiastočného odstránenia chyby. Po jej preradení začína plynúť nový čas na odstránenie chyby príslušný pre novú kategóriu chyby, do ktorej bola chyba preradená.

6. Poskytovateľ nezodpovedá objednávateľovi za nedostatky spôsobené konaním alebo opomenutím tretích strán, napr. výpadok el. sieti, resp. chyby spôsobené v dôsledku výpadku el. siete, výpadok internetového spojenia, resp. chyby spôsobené v dôsledku výpadku int. spojenia a pod, resp. za nedodržanie podmienok užívania informačných systémov, resp. softvéru. Odstraňovanie takýchto chýb sa považuje ako naviac práca, ak sa zmluvné strany nedohodli inak.

VII. DÔSLEDKY NEPLNENIA ZMLUVY, ZMLUVNÉ POKUTY

1. Zmluvné strany si pre prípad porušenia povinností vyplývajúcich z tejto zmluvy dohodli nasledovné zmluvné pokuty:

1.1 Ak poskytovateľ nedodrží ustanovenia zmluvy týkajúce sa poskytnutia služby v jednotlivých častiach predmetu zmluvy alebo odstránenia chyby, zaplatí zmluvnú pokutu vo výške 0,05 % z ceny príslušnej časti predmetu zmluvy, z ktorej vykonaním je v omeškaní za každý aj začatý kalendárny deň omeškania, maximálne však do výšky 10% predmetu ceny plnenia, to neplatí v prípade, ak poskytovateľ z objektívnych dôvodov, ktoré sám nespôsobil (*napr. včasné nevydanie vykonávacích predpisov, usmernení, vyhlášok, nariadení a/alebo iné v prípade ak sa má vykonať legislatívny update*), alebo ak nastal niektorý z dôvodov vyššej moci a teda, ak nastanú vážne objektívne dôvody, v dôsledku ktorých nebude môcť poskytovateľ poskytovať služby v zmysle tejto zmluvy. Vážnymi objektívnymi dôvodmi podľa predchádzajúcej vety sú predovšetkým mimoriadne, nepredvídateľné, neodvrátiteľné a nezavinené udalosti, ktoré nastali nezávisle od vôle poskytovateľa, ak nemožno rozumne predpokladať, že by poskytovateľ tieto prekážky alebo ich následky vedel prekonať alebo odvrátiť, ktorými sú predovšetkým neodvrátiteľné živelné udalosti alebo neovplyvniteľné štátom nariadené opatrenia (nariadenia), na základe ktorých dôjde k zákazu alebo podstatnému obmedzeniu prevádzkovania niektorej činností poskytovateľa, ktorá objektívne znemožní plnenie jeho povinností podľa tejto zmluvy.

1.2 Ak objednávateľ nezaplatí vyfakturovanú zmluvnú cenu v lehote splatnosti, zaplatí zmluvnú pokutu vo výške 0,05 % z ceny s ktorou je v omeškaní a to za každý aj začatý kalendárnych deň omeškania, maximálne však do výšky 10% predmetu ceny plnenia.

1.3 Odhliadnuc od znenia ods. 1.2 tohto článku zmluvy je poskytovateľ v prípade omeškania objednávateľa s úhradou jednotlivých faktúr poskytovateľa, oprávnený prerušiť poskytovanie plnenia na základe tejto zmluvy až do riadnej úhrady faktúr objednávateľom, pričom takéto prerušenie poskytovania plnenia sa nepovažuje za omeškanie na strane poskytovateľa, resp. porušenie ustanovení tejto zmluvy.

1.4 Lehota splatnosti faktúr, ktorými sa uplatňujú zmluvné pokuty je do 14 kalendárnych dní odo dňa ich doručenia.

2. Dojednaním zmluvnej pokuty nie je dotknutý nárok na náhradu skutočnej priamej škody, ktorá vznikla porušením zmluvnej povinnosti, na ktorú sa vzťahuje zmluvná pokuta vo výške presahujúcu zmluvnú pokutu, maximálne však do výšky 10% ceny predmetu plnenia v zmysle čl. III. tejto zmluvy pre jeden kalendárny rok poskytovania podpory.
3. Celkové finančné záväzky, ktoré bude poskytovateľ znášať v súvislosti so všetkými nárokmi vznesenými v súvislosti s touto Zmluvou, nepresiahnu hodnotu skutočných priamych škôd, ktoré vzniknú objednávateľovi.

VIII. ZÁVEREČNÉ USTANOVENIA

1. Zmluva nadobúda platnosť dňom jej podpísania obidvomi zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia podľa § 47a Občianskeho zákonníka, nie však skôr ako 1.1.2024.
2. Ostatné náležitosti neupravené touto zmluvou sa primerane riadia ustanoveniami Obchodného zákonníka a Autorského zákona.
3. Zmluva môže zaniknúť:
   3.1 dohodou zmluvných strán
   3.2 odstúpením od zmluvy ktorejkoľvek zmluvnej strany, ak druhá strana poruší ustanovenia tejto zmluvy podstatným spôsobom.
   3.3 písomnou výpoveďou bez udania dôvodu, a to ku koncu kalendárneho štvrťroka, pričom výpovedná doba je 3 mesiace a začína plynúť od začiatku štvrťroku nasledujúceho po štvrťroku, v ktorom bola protistrane výpoveď doručená.
4. Neoddeliteľnou súčasťou tejto zmluvy sú prílohy
   - Príloha č. 1 **Rekapitulácia ceny služieb za obdobie kalendárneho roka**
   - Príloha č. 2 **Užšia špecifikácia predmetu plnenia**
   - Príloha č. 3 **Technická špecifikácia na rok 2024**
   - Príloha č. 4 **Bezpečnostné opatrenia a iné povinnosti** vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášku Národného bezpečnostného úradu č. 362/2018 Z.z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrenia.
   - Príloha č.5 **Zoznam subdodávateľov**
5. Táto zmluva je vyhotovená v 4 (štyroch) exemplároch, z ktorých 2 (dva) obdrží objednávateľ a 2 (dva) z poskytovateľ.
6. Meniť alebo dopĺňať obsah zmluvy je možné pri dodržaní § 18 zákona č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, len formou písomných očíslovaných dodatkov, ktoré budú platné, ak budú riadne potvrdené a podpísané oprávnenými zástupcami oboch zmluvných strán a účinné dňom nasledujúcim po dni zverejnenia.
7. V prípade rozporu medzi ustanoveniami zmluvy a dispozitívnymi ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, platia ustanovenia zmluvy. V prípade rozporu medzi ustanoveniami zmluvy a ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, ktoré je možné dohodou zmluvných strán vylúčiť, platia ustanovenia zmluvy a uvedené

ustanovenia všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky sa považujú za výslovne vylúčené.

8. Ak niektoré ustanovenia tejto zmluvy sú neplatné alebo po jej podpise stratia platnosť, nie je tým dotknutá platnosť a účinnosť ostatných ustanovení tejto zmluvy. Namiesto neplatných alebo neúčinných ustanovení tejto zmluvy alebo na úpravu právnych vzťahov, ktoré nie sú touto zmluvou upravené, sa použijú ustanovenia zákona č. 513/1991 Zb. Obchodný zákonník, ktoré sú obsahom a účelom najbližšie obsahu a účelu tejto zmluvy.
9. Zmluvné strany vyhlasujú, že ustanoveniam tejto zmluvy porozumeli, že táto zmluva bola uzavretá určite, vážne a zrozumiteľne, na základe ich pravej a slobodnej vôle, nie v tiesni a za nápadne nevýhodných podmienok, na znak čoho ju podpisujú.

Dátum ..... Dátum .....

PhDr. Mgr. Ján Ferenčák, MBA

primátor mesta

objednávateľ poskytovateľ

PRÍLOHA Č. 1

REKAPITULÁCIA CENY SLUŽIEB NA OBDOBIE KALENDÁRNEHO ROKA

Počet jednotiek	Jednotka	Cena za jednotku bez DPH	Cena Spolu bez DPH	Cena Spolu s DPH
Údržba licencií dodaného licenčného softvéru				
1	celok	1 200,00 €	1 200,00 €	1 440,00 €
UPDATE – Údržba licencií dodaného aplikačného softvéru				
1	celok	29 667,00 €	29 667,00 €	35 600,40 €
UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru				
50	ČH	89,00 €	4 450,00 €	5 340,00 €
HotLine podpora				
60	ČH	85,00 €	5 100,00 €	6 120,00 €
Riadenie projektu				
32	ČH	84,00 €	2 688,00 €	3 225,60 €
Technická podpora				
16	ČH	124,38 €	1 990,00 €	2 388,00 €
Metodická podpora				
40	ČH	98,13 €	3 925,00 €	4 710,00 €
Školenia/metodické dni				
10	osoba/školenie	98,00 €	980,00 €	1 176,00 €
Bezpečnostná politika				
1	celok	1 990,00 €	1 990,00 €	2 388,00 €

PRÍLOHA Č. 2

Užšia špecifikácia predmetu plnenia

Na určenie rozsahu služieb sa v rámci tejto zmluvy používajú nasledovné skratky:

- ČD = človeko-deň, 1 ČD = 8 hodín pracovného času,
- ČH = človeko-hodina, 1 ČH = 60 minút pracovného času.

UPDATE – Údržba licencií dodaného aplikačného softvéru

- Kontrola log súborov verzií (3 verzie ročne) a kumulatívnych zmien (3 plánované kumulatívne zmeny ročne) vyplývajúce z legislatívy. Pre vylúčenie pochybnosti platí, že poskytovateľ je povinný vykonať legislatívny update najneskôr do 90 dní potom, čo budú zo strany príslušného orgánu verejnej moci sprístupnené (zverejnené) všetky relevantné technické podmienky a požiadavky na vykonanie predmetného legislatívneho updatu (tzn. všetky relevantné vykonávacie predpisy, usmernenia, vyhlášky, nariadenia a/alebo iné dokumenty).

UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru

- UPGRADE bude dodávaný vo forme verzií, pričom ročne budú vydané minimálne 3 verzie v súlade s verziami UPDATE. Špecifické analytické a programátorské práce môžu byť dodané aj inou formou ako v rámci verzie na základe vzájomnej dohody zmluvných strán.
- Služby spojené s napĺňaním informačného systému údajmi, čo zahŕňa celý životný cyklus spracovania údajov: príprava, transformácia, migrácia, čistenie a import údajov.
- Dodanie priestorových údajov záujmových území objednávateľa a súvisiacich služieb za účelom ich využitia v informačnom systéme objednávateľa.
- Pod pojmom priestorové údaje sa pre účely tejto zmluvy rozumejú digitálne geodetické údaje vytvorené spracovaním analógových alebo digitálnych podkladov katastrálnych území pre intravilán a extravilán obcí do elektronickej formy podľa dohodnutej štruktúry. Priestorové dáta sú spracované v súradnicovom systéme S-JTSK.
- Požiadavky objednávateľa budú evidované v CG HelpDesku. Požiadavka, ktorá bude poskytovateľom potvrdená, bude zaradená do výrobného plánu. Informáciu o zaradení do verzie nájde objednávateľ v aplikácii CG HelpDesk. Objednávateľ má právo požiadať o prehodnotenia zaradenia požiadavky do verzie.
- Požiadavka sa poskytovateľom posudzuje nasledovne:
  - Reakčná doba na požiadavku je 5 pracovných dní od jej zaevidovania. Počas reakčnej doby bude objednávateľ informovaný o prijatí požiadavky a jej zaradení do procesu posudzovania.
  - Návrh riešenia požiadavky poskytovateľ oznámi objednávateľovi do 50 pracovných dní od prijatia požiadavky a jej zaradenia do procesu posudzovania. K predloženému návrhu je objednávateľ povinný sa vyjadriť v lehote 30 kalendárnych dní od doručenia návrhu riešenia požiadavky objednávateľovi. V opačnom prípade sa návrh poskytovateľa pokladá za akceptovaný objednávateľom.
  - V prípade zamietnutia návrhu objednávateľom má poskytovateľ právo odčerpať 16 ČH z položky UPGRADE.
  - Termín realizácie a dodania odsúhlasenej požiadavky je stanovený v rámci najbližšej plánovanej verzie ASW, ktorá nasleduje po lehote 90 kalendárnych dní od dátumu odsúhlasenia požiadavky objednávateľom.

Riadenie projektu

- Pre objednávateľa plní zadania vyplývajúce z rozvojových aktivít v oblasti informačných technológií a to formou poradenstva, vypracovávaním štúdií dopadov zavádzania inovatívnych riešení ako aj priamym konzultovaním s potenciálnymi partnermi objednávateľa v tejto oblasti.
- Pôsobí v pozícii poradcu pre rozvoj SW a HW infraštruktúry v prostredí IKT objednávateľa. Jeho kladné stanovisko je potrebné v prípade implementácie SW, ktorý má priamu interakciu s riešeniami zmysle tejto zmluvy a ich rozšírení.

- Dodávateľom stanovuje podmienky, za ktorých je možná prevádzka novo implementovaných riešení, ktoré nemajú priamu interakciu, ale ich výstup je súčasťou spoločného výstupu s ostatnými výstupmi.
- Rieši optimalizáciu prostredia s cieľom úspor výpočtových, kapacitných ako aj ekonomických parametrov prevádzkovaných IT s ohľadom na optimálny návrh procesov informačných systémov.
- Koordinácia aktivít súvisiacich s technickou podporou, serverové riešenia.
- Minimálne čerpanie služby je v rozsahu 0,5 ČH z pracoviska poskytovateľa a 8 ČH u objednávateľa.

Technická podpora
- Minimálne čerpanie služby je v rozsahu 0,5 ČH z pracoviska poskytovateľa a 8 ČH u objednávateľa.

Metodická podpora
- Minimálne čerpanie služby v rozsahu 4 ČH z pracoviska poskytovateľa a 8 ČH u objednávateľa.
- V prípade čerpania služby nad 40 ČH sa objednávateľ zaväzuje dodatočne objednať metodickú podporu, pričom cena za každú začatú ČH nad rámec 8 ČH bude započítaná ako dvojnásobok cenníkovej ceny 1 ČH metodickej podpory.

Školenia/metodické dni
- Poskytovateľ ponúkne objednávateľovi vždy dva termíny na realizáciu školení v školiacom stredisku poskytovateľa. V prípade, že žiaden z týchto termínov nebude objednávateľovi vyhovovať, bude mu umožnené zúčastniť sa iných školení, ktoré sa budú realizovať v ostatných školiacich strediskách poskytovateľa. Poskytovateľ je zodpovedný za prípravu školiacej miestnosti a má právo zrušiť vyhlásený termín školenia v prípade nedostatočnej účasti zákazníkov (menej ako 5 účastníkov).
- Minimálne čerpanie služby v rozsahu 1 účastník školenia na 1 deň u poskytovateľa (za účasť jednej osoby na Metodickom dni informatikov (MDI) a na konferencii CGIT bude rozsah ponížený o dvoch účastníkov školenia).

Podmienky realizácie služieb:

- V prípade zrušenia dohodnutého termínu realizácie vybraných služieb (technická podpora, metodická podpora alebo školenie), potvrdeného zástupcami vo veciach technických oboch zmluvných strán, z dôvodov na strane objednávateľa menej ako 7 pracovných dní pred ich uskutočnením, je výška storno poplatku 100 % z ceny služby, teda poskytovateľ si bude účtovať náklady súvisiace s týmito nezrealizovanými službami v takej výške, ako keby sa služby boli zrealizovali a má sa za to, že služba bola realizovaná v súlade so zmluvou.
    - V prípade potreby vykonania služieb/ podpory v sídle objednávateľa vo viaceré dni za sebou nasledujúce, má poskytovateľ nárok na náhradu za ubytovanie vo výške 100 EUR/osoba/noc

PRÍLOHA Č. 3

TECHNICKÁ ŠPECIFIKÁCIA NA ROK 2024

Systémové požiadavky pre klienta aplikácie CG ISS

V prípade použitia základného klienta CG ISS na terminálovom serveri Microsoft je možné použiť ako terminálový server serverový operačný systém 2016, 2019, 2022 v edíciách Standard, Datacenter. Pri použití iného typu a verzie terminálového servera nás pre potvrdenie funkčnosti kontaktujte.

Hardvér, softvér	Klient CG ISS minimálna konfigurácia	Klient CG ISS odporúčaná konfigurácia
procesor	2,0 GHz a vyšší	2,8 GHz a vyšší
RAM	2 GB	4 GB
HDD	40 GB viac	80 GB a viac
LAN	100 Mbit	1 Gbit
VGA	min. 64 MB VRAM	min. 128 MB VRAM
monitor	19“ LCD / CRT, rozlíšenie 1024 x 768	21“ až 24“ LCD, rozlíšenie 1920 x1080
*Platforma	Windows 10 Pro, 11 Pro	Windows 10 Pro (x64)
**Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge, Mozilla Firefox, Google Chrome
Softvér	Oracle klient 11gR2 32-bit Runtime IS 3.2	Oracle klient 11gR2 32-bit Runtime IS 3.2
Softvér pre prepojenie na CG GISAM	MS SOAP Toolkit 3.0 SDK	MS SOAP Toolkit 3.0 SDK
Softvér pre prepojenie na REGOB	MS SOAP Toolkit 3.0 SDK Microsoft .NET Framework 3.5 SP1	MS SOAP Toolkit 3.0 SDK Microsoft .NET Framework 3.5 SP1
***Kancelársky softvér	MS Office 2016, 2019	MS Office 2016, 2019
****Softvér pre elektronizáciu	Aplikácie pre KEP/ZEP (D.Suite/eIDAS)	Aplikácie pre KEP/ZEP (D.Suite/eIDAS)
Iný softvér	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.7.2/4.8 MS SOAP Toolkit SDK 3.0 Acrobat Reader 9.x alebo noší MS XML 4.0, 6.0	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.7.2 MS SOAP Toolkit SDK 3.0 Acrobat Reader 9.x alebo novší MS XML 4.0, 6.0

** V prípade požiadaviek na použitie 64 bitového systému, nás pre potvrdenie funkčnosti kontaktujte. Môžu byť použité aj iné edície vhodné OS pre firemné prostredie (Ultimate, Enterprise).*

*** V prípade použitia zabudovaného prehliadača Chromium je potrebné postupovať podľa inštrukcií dodávateľa.*

**** V prípade požiadaviek na použitie iného softvéru (internetový prehliadača, kancelársky softvér MS Office 2022, OpenOffice a pod.) pre potvrdenie funkčnosti kontaktujte dodávateľa.*

***** Softvér je dostupný na stránkach www.slovensko.sk v sekcii na stiahnutie.*

Systémové požiadavky pre klientov aplikácií CG Portál ISS, CG GISAM, CG DISS

V prípade použitia aplikácií na terminálovom serveri Microsoft je možné použiť ako terminálový server serverový operačný systém 2019, 2022 v edíciách Standard, Datacenter. Pri použití iného typu a verzie terminálového servera nás pre potvrdenie funkčnosti kontaktujte.

Hardvér, softvér	**Klient CG Portál ISS Klient CG GISAM Klient CG DISS minimálna konfigurácia**	**Klient CG Portál ISS Klient CG GISAM Klient CG DISS odporúčaná konfigurácia**
procesor	2,0 GHz a vyšší	2,8 GHz a vyšší
RAM	1 GB	2 GB alebo viac
HDD	60 GB viac	80 GB a viac
LAN	100 Mbit	1 Gbit
VGA	min. 128 MB VRAM	min. 128 MB VRAM
monitor	19“ LCD / CRT, rozlíšenie 1024 x 768	21“ až 24“ LCD, rozlíšenie 1920 x1080
*Platforma	Windows 10 Pro, 11 Pro	Windows 10 Pro (x64)
**Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge,Mozilla Firefox, Google Chrome
**Kancelársky softvér	MS Office 2019	MS Office 2019
Softvér pre skener	Softvér dodaný výrobcom skenera	Softvér dodaný výrobcom skenera
***Softvér pre elektronizáciu	Ovládač na čítačku čipových kariet Aplikácia na prihlásenie (eID klient) Aplikácie pre KEP/ZEP (D.Suite/eIDAS)	Ovládač na čítačku čipových kariet Aplikácia na prihlásenie (eID klient) Aplikácie pre KEP/ZEP (D.Suite/eIDAS)
Iný softvér	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.7.2 / 4.8 Acrobat Reader 9.x alebo novší MS SOAP Toolkit SDK 3.0 MS XML 4.0 a vyšší	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.7.2 Acrobat Reader 9.x alebo novší MS SOAP Toolkit SDK 3.0 MS XML 4.0 a vyšší

** V prípade požiadaviek na použitie 64 bitového systému, nás pre potvrdenie funkčnosti kontaktujte. Môžu byť použité aj iné edície vhodné OS pre firemné prostredie (Ultimate, Enterprise).*
*** V prípade požiadaviek na použitie iného softvéru (internetový prehliadač, kancelársky softvér MS Office 2022, OpenOffice a pod.) nás pre potvrdenie funkčnosti kontaktujte.*
**** Softvér je dostupný na stránkach www.slovensko.sk v sekcii na stiahnutie.*

Skener pre CG DISS	
Parameter	**Hodnota**
Optické rozlíšenie skenovania	4 800 dpi a viac
Rozlíšenie pri hardvérovom skenovaní	800 x 4 800 DPI
Bitová hĺbka	48-bitov a viac
Skenovacie režimy	farebný, odtiene šedej, čiernobiely
Skenované formáty	A5, A4, prípadne menšie rozmery bezokrajové skenovanie
*OCR	Možnosť rozpoznávania slovenského jazyka v texte
Iné požiadavky	Prechodové snímanie, obojstranné snímanie Podpora ukladania výstupu do PDF, JPG/PNG Možnosť ukladania preddefinovaných skenovacích profilov
Pripojiteľnosť	USB, LPT, LAN
Kapacita automatického podávača dokumentov	Štandardná, 50 listov

** Len v prípade, že sa plánuje využívať.*

Skenovací program pre CG DISS
V prípade použitia na OS je možné aplikáciu používať v prehliadači MS Edge. Pre bližšie informácie nás kontaktujte.

Systémové požiadavky pre server aplikácie CG ISS

Server pre CG ISS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon. Je nutné konzultovať dopad na prevádzkované aplikácie s dodávateľom CORA GEO, s.r.o. v prípade:

- využitia diskov SATA a NL SATA namiesto SAS,
- využitia serverov prevádzkovaných vo virtuálnom prostredí,
- využitia novej verzie LSW s overením podpory a kompatibility,
- použitia serverov v konfigurácii s minimálnymi požiadavkami,
- využitia existujúcich serverov alebo súčasnej prevádzky iných informačných systémov a rolí OS na serveri,
- využitia iného OS pre databázový server.

Požiadavky na sieťové prostredie pre CG ISS:

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps, odporúčané 1 Gpbs
- server pripojený na 1 Gpbs,
- doména Windows alebo pracovná skupina,
- administrátorský prístup na server,
- používateľské účty pre správu a implementáciu produktov,
- na serveri s projektom a databázou CG ISS:
    - povolené porty pre komunikáciu klient/server pre projekt CG ISS (zdieľanie),
    - povolená komunikácia klient/server na Oracle databázový server (štandardne port TCP 1521),
    - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
    - v prípade využívania služieb CoraInfo povolená komunikácia na https://info.corageo.sk,
    - v prípade využívania služieb CGMS povolená komunikácia na https://cgms.corageo.sk a zriadenie mailovej schránky pre odosielanie správ, ak je využívané (zvyčajne espravy@domena.sk),
- na klientoch povolený prístup k projektu a databáze CG ISS (firewall, MS Edge).

Hardvérové a softvérové požiadavky pre server CG ISS

Hardvér/ softvér	Server CG ISS minimálne požiadavky	Server CG ISS odporúčané požiadavky
*procesor	2 x CPU Dual Core 3,0 GHz a viac alebo 2 x CPU Quad/Hexa Core	2 x CPU Quad Core s možnosťou rozšírenia na viac CPU
**RAM	8 GB s max. kapacitou aspoň 32 GB	12 GB a viac s max. kapacitou aspoň 32 GB
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	Integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS pre projekt CG ISS a databázu SAS/SATA pre zálohy, otáčky 10k alebo 15k	SAS pre projekt CG ISS a databázu SAS/SATA pre zálohy, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***100 - 300 GB v RAID1/10/5/6 pre údaje ***200 - 300 GB v RAID1/5/6 pre zálohy	60 GB v RAID1/10/5/6 pre OS ***100 - 300 GB v RAID1/10/5/6 pre údaje ***200 - 300 GB v RAID1/5/6 pre zálohy
LAN	1 Gbps	2 x 1 Gbps
Zálohovacie zariadenie	Pásková mechanika LTO4 a viac, sieťový disk, externý USB disk, a pod.	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.
UPS	Riadený záložný zdroj na 15 až 30 min.	Riadený záložný zdroj na 15 až 30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
Databáza	Oracle RDBMS 11gR2	Oracle RDBMS 11gR2
****Operačný systém	Windows Server 2019, 2022	Windows Server 2019, 2022
*****Softvér	MS Edge,Mozilla Firefox, Google Chrome Runtime IS, Oracle klient 11gR2 32-bit	MS Edge,Mozilla Firefox, Google Chrome Runtime IS, Oracle klient 11gR2 32-bit

** Môžu byť použité ekvivalenty virtuálnych CPU.*
*** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.*
**** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.*
***** Podporované edície Standard, Datacenter*
****** V prípade použitia zabudovaného prehliadača Chromium je potrebné postupovať podľa inštrukcií dodávateľa.*

Požiadavky pre súčasnú prevádzku CG Portál ISS a CG GISAM

Odporúča sa aplikácie CG Portál ISS a CG GISAM prevádzkovať na samostatnom serveri, nie

spoločne na serveri s CG ISS.

Softvér/hardvér	Server CG ISS + CG Portál ISS	Server CG ISS + CG GISAM
RAM	-	+ 4 GB
Webový server	Microsoft IIS na podporovanom OS	Microsoft IIS na podporovanom OS
Oracle AS	-	Oracle GlassFish 3.2, Oracle Mapviewer 11g
Softvér	MS .NET Framework 3.5 MS .NET Framework 4.7.2	MS .NET Framework 3.5 MS .NET Framework 4.7.2 MS SOAP Toolkit 3.0 Java JDK 1.8 64-bit

Požiadavky pre súčasnú prevádzku s CG DISS

Odporúča sa aplikácie CG DISS prevádzkovať na samostatnom serveri, nie spoločne na serveri s CG ISS, môže byť použitý server CG Portál ISS a CG GISAM.

Softvér/hardvér	Server CG ISS + CG DISS
RAM	+ 1 GB
Webový server	Microsoft IIS na podporovanom OS
Softvér	MS .NET Framework 3.5 MS .NET Framework 4.7.2
*Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome

** V prípade požiadaviek na použitie iného internetového prehliadača nás pre potvrdenie funkčnosti kontaktujte.*

Systémové požiadavky pre server CG Portál ISS

Server CG Portál ISS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon. Predpokladá sa využívanie spoločnej databázy s aplikáciou CG ISS. Je nutné konzultovať dopad na prevádzkované aplikácie s dodávateľom CORA GEO, s.r.o. v prípade:

- využitia diskov SATA a NL SATA namiesto SAS,
- využitia serverov prevádzkovaných vo virtuálnom prostredí,
- využitia novej verzie LSW s overením podpory a kompatibility,
- použitia serverov v konfigurácii s minimálnymi požiadavkami,
- využitia existujúcich serverov alebo súčasnej prevádzky iných informačných systémov a rolí OS na serveri,
- využitia iného OS pre databázový server.

1. Hardvérové a softvérové požiadavky pre server CG Portál ISS

Hardvér/ softvér	Server CG Portál minimálne požiadavky	Server CG Portál odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	2 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	1 Gbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15 až 30 min.	Riadený záložný zdroj na 15 až 30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2016, 2019, 2022	Windows Server 2019, Windows Server 2022
Oracle klient	Oracle klient 11gR2 32-bit	Oracle klient 11gR2 32-bit
Web server	Microsoft IIS na podporovanom OS	Microsoft IIS na podporovanom OS
Softvér	MS .NET Framework 3.5 + 4.7.2 / 4.8 Acrobat Reader 9.x alebo novší	MS .NET Framework 3.5 + 4.7.2 Acrobat Reader 9.x alebo novší
*****Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge, Mozilla Firefox, Google Chrome

** Môžu byť použité ekvivalenty virtuálnych CPU.*
*** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.*
**** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.*
***** Podporované edície Standard, Datacenter.*
****** V prípade požiadaviek na použitie iného internetového prehliadača nás pre potvrdenie funkčnosti kontaktujte.*

2. Požiadavky na sieťové prostredie pre CG Portál ISS

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps, odporúčané 1 Gpbs,
- server pripojený na 1 Gpbs,
- doména Windows alebo pracovná skupina,
- administrátorský prístup na server,
- používateľské účty pre správu a implementáciu produktov,
- mailové konto s povolením zasielania mailov cez SMTP aj mimo lokálnu poštovú doménu (zvyčajne portal@domena.sk) pre účely zasielania servisných správ,
- na serveri s CG Portál ISS:
    - povolené porty pre komunikáciu aplikačného servera CG Portál ISS,
    - povolené porty pre komunikáciu webového servera Microsoft IIS (http, https) aj z LAN,
    - povolená komunikácia na Oracle databázový server (TCP 1521),
    - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
    - v prípade využívania služieb CoraInfo povolená komunikácia na https://info.corageo.sk,

- na klientoch povolený a nakonfigurovaný prístup k webovej aplikácii CG Portál ISS (firewall, MS Edge, proxy server).

Systémové požiadavky pre CG GISAM

Server pre CG GISAM môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon. Predpokladá sa využívanie spoločnej databázy s aplikáciou CG ISS. Je nutné konzultovať dopad na prevádzkované aplikácie s dodávateľom CORA GEO, s.r.o. v prípade:

- využitia diskov SATA a NL SATA namiesto SAS,
- využitia serverov prevádzkovaných vo virtuálnom prostredí,
- využitia novej verzie LSW s overením podpory a kompatibility,
- použitia serverov v konfigurácii s minimálnymi požiadavkami,
- využitia existujúcich serverov alebo súčasnej prevádzky iných informačných systémov a rolí OS na serveri,
- využitia iného OS pre databázový server.

1. Hardvérové a softvérové požiadavky pre server CG GISAM

Hardvér/ softvér	Server CG GISAM minimálne požiadavky	Server CG GISAM odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	1 Gbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15 až 30 min.	Riadený záložný zdroj na 15 až 30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2016, 2019, 2022	Windows Server 2019, 2022
Softvér Oracle	Oracle GlasFish 3.2, Oracle Mapviewer 11g, Oracle Mapbuilder 11g, Oracle klient 11gR2 32-bit	Oracle GlasFish 3.2, Oracle Mapviewer 11g, Oracle Mapbuilder 11g, Oracle klient 11gR2 32-bit
Web server	Microsoft IIS na podporovanom OS	Microsoft IIS na podporovanom OS
Softvér	Java JDK 1.8 (x64), MS SOAP Toolkit 3.0 MS .NET Framework 3.5 a 4.7.2 / 4.8 Acrobat Reader 9.x alebo novší	Java JDK 1.8 (x64), MS SOAP Toolkit 3.0 MS .NET Framework 3.5 a 4.7.2 Acrobat Reader 9.x alebo novší

*****Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge, Mozilla Firefox, Google Chrome

** Môžu byť použité ekvivalenty virtuálnych CPU.*

*** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.*

**** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.*

***** Podporované edície Standard, Datacenter.*

****** V prípade požiadaviek na použitie iného internetového prehliadača nás pre potvrdenie funkčnosti kontaktujte.*

2. Požiadavky na sieťové prostredie pre CG GISAM

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps, odporúčané 1 Gpbs,
- server pripojený na 1 Gpbs,
- doména Windows alebo pracovná skupina,
- používateľské účty pre správu a implementáciu produktov,
- administrátorský prístup na server,
- na serveri s CG GISAM:
    - povolené porty pre aplikačný server Oracle (TCP 9200-9202),
    - povolená komunikácia klientov na aplikačný server Oracle (TCP 9200) v LAN,
    - povolené porty pre komunikáciu webového servera Microsoft IIS (http, https),
    - povolené porty pre komunikáciu s aplikačným serverom CG Portál ISS,
    - povolená komunikácia na Oracle databázový server (TCP 1521),
    - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
    - v prípade využívania služieb CoraInfo povolená komunikácia na https://info.corageo.sk,
- na klientoch povolený a nakonfigurovaný prístup k intranetovej webovej aplikácii CG GISAM (firewall, MS Edge, proxy server).

Systémové požiadavky pre server CG DISS

Server CG DISS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon. Predpokladá sa využívanie spoločnej databázy s aplikáciou CG ISS. Je nutné konzultovať dopad na prevádzkované aplikácie s dodávateľom CORA GEO, s.r.o. v prípade:

- využitia diskov SATA a NL SATA namiesto SAS,
- využitia serverov prevádzkovaných vo virtuálnom prostredí,
- využitia novej verzie LSW s overením podpory a kompatibility,
- použitia serverov v konfigurácii s minimálnymi požiadavkami,
- využitia existujúcich serverov alebo súčasnej prevádzky iných informačných systémov a rolí OS na serveri.

1. Hardvérové a softvérové požiadavky pre server CG DISS

Hardvér/ softvér	Server CG DISS minimálne požiadavky	Server CG DISS odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	1 Gbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15 až 30 min.	Riadený záložný zdroj na 15 až 30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2019, 2022	Windows Server 2019 Windows Server 2022
Oracle klient	Oracle klient 11gR2 32-bit	Oracle klient 11gR2 32-bit
Web server	Microsoft IIS na podporovanom OS	Microsoft IIS na podporovanom OS
Softvér	MS .NET Framework 3.5 + 4.7.2/4.8 Acrobat Reader 9.x alebo novší	MS .NET Framework 3.5 + 4.7.2 Acrobat Reader 9.x alebo novší
Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge, Mozilla Firefox, Google Chrome

** Môžu byť použité ekvivalenty virtuálnych CPU.*
*** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.*
**** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.*
***** Podporované edície Standard, Datacenter a verzie oper.systémov, ktoré sú aktuálne podporované výrobcom.*

Požiadavky na sieťové prostredie pre CG DISS

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps, odporúčané 1 Gpbs,
- server pripojený na 1 Gpbs,
- doména Windows,
  POZN: Využívanie aplikácie v prostredí pracovnej skupiny je nutné konzultovať s dodávateľom.
- administrátorský prístup na server,
- používateľské účty pre správu a implementáciu produktov,

- v prípade využívania notifikácie mailové konto s povolením zasielania mailov cez SMTP aj mimo lokálnu poštovú doménu, zvyčajne edis@domena.sk,
- na serveri s CG DISS
    - povolené porty pre komunikáciu webového servera Microsoft IIS (http, https) aj z LAN,
    - povolená komunikácia na Oracle databázový server (TCP 1521),
    - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
    - pre aplikáciu prevádzkovanú na protokole https vystavený SSL certifikát na meno servera a dôveryhodný v prostredí domény Windows,
    - v prípade využívania služieb CoraInfo povolená komunikácia na https://info.corageo.sk,
- na klientoch povolený a nakonfigurovaný prístup k intranetovej webovej aplikácii CG DISS (firewall, MS Edge, proxy server).

Systémové požiadavky pre CG WEBGIS

Server pre CG WEBGIS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon. Je nutné konzultovať dopad na prevádzkované aplikácie s dodávateľom CORA GEO, s.r.o.:

- využitia diskov SATA a NL SATA namiesto SAS,
- využitia serverov prevádzkovaných vo virtuálnom prostredí,
- využitia novej verzie LSW s overením podpory a kompatibility,
- použitia serverov v konfigurácii s minimálnymi požiadavkami,
- využitia existujúcich serverov alebo súčasnej prevádzky iných informačných systémov a rolí OS na serveri,
- využitia iného OS pre databázový server.

1. Hardvérové a softvérové požiadavky pre server CG WEBGIS

Hardvér/ softvér	Server CG WEBGIS minimálne požiadavky	Server CG WEBGIS odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	2x 100 Mbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15 až 30 min.	Riadený záložný zdroj na 15 až 30 min.
Zálohovacie zariadenie	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2019, 2022	Windows Server 2019, 2022
Databáza	Oracle RDBMS 11gR2	Oracle RDBMS 11gR2
Softvér Oracle	Oracle GlasFish 3.2 Oracle Mapviewer 11g Oracle Mapbuilder 11g Oracle klient 11gR2 32-bit	Oracle GlasFish 3.2 Oracle Mapviewer 11g Oracle Mapbuilder 11g Oracle klient 11gR2 32-bit
Web server	Microsoft IIS na podporovanom OS	Microsoft IIS na podporovanom OS
Softvér	Java JDK 1.8 (x64) MS .NET Framework 3.5 MS .NET Framework 4.7.2/4.8 Acrobat Reader 9.x alebo novší	Java JDK 1.8 (64-bit) MS .NET Framework 3.5 MS .NET Framework 4.7.2 Acrobat Reader 9.x alebo novší
Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge, Mozilla Firefox, Google Chrome

** Môžu byť použité ekvivalenty virtuálnych CPU.*

*** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.*
**** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.*
***** Podporované edície Standard, Datacenter*

Požiadavky na sieťové prostredie pre CG WEBGIS

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps, odporúčané 1 Gpbs,
- server pripojený 1 Gpbs v DMZ, prípadne 1 x LAN 1 Gbps, 1 x Internet 100 Mbps,

  POZN: Možnosti reálneho zapojenia závisia od sieťovej infraštruktúry a použitých prvkov (firewall, proxy servera pod.) na úrade a je možné ich čiastočne prispôsobiť.

- pevná internetová adresa,
- registrované internetové DNS záznamy typu A napr. gis.domena.sk a syncgis.domena.sk,
- na firewalle a proxy serveri zabezpečiť smerovania dotazov z LAN a Internetu na http://gis.domena.sk prípadne https://gis.domena.sk. na vnútornú adresu servera bez zmeny hlavičky s použitím host header,
- používateľské účty pre správu a implementáciu produktov,
- administrátorský prístup na server,
- na serveri s CG WEBGIS
  - povolené porty pre aplikačný server Oracle (TCP 9200-9202),
  - povolené porty pre komunikáciu webového servera Microsoft IIS (http, https),
  - povolená komunikácia na Oracle databázový server (TCP 1521),
  - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
  - v prípade využitia SSL zakúpený SSL certifitkát typu SHA256 od dôveryhodnej internetovej certifikačnej autority pre daný internetový DNS, prípadne iný napr. typu wildcard (*.domena.sk),
  - v prípade využívania služieb CoraInfo povolená komunikácia na https://info.corageo.sk,
- povolená komunikácia servera do siete Internet (80, 443).

Systémové požiadavky pre CG EGOV

Server pre CG EGOV môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon. Je nutné konzultovať dopad na prevádzkované aplikácie s dodávateľom CORA GEO, s.r.o. v prípade:

- využitia diskov SATA a NL SATA namiesto SAS,
- využitia serverov prevádzkovaných vo virtuálnom prostredí,
- využitia novej verzie LSW s overením podpory a kompatibility,
- použitia serverov v konfigurácii s minimálnymi požiadavkami,
- využitia existujúcich serverov alebo súčasnej prevádzky iných informačných systémov a rolí OS na serveri,
- využitia iného OS pre databázový server.

1. Hardvérové a softvérové požiadavky pre server CG EGOV

Hardvér/ softvér	Server CG EGOV minimálne požiadavky	Server CG EGOV odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	2 x 100 Mbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15 až 30 min.	Riadený záložný zdroj na 15 až 30 min.
Zálohovacie zariadenie	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2016, 2019, 2022	Windows Server 2019 Windows Server 2022
Databáza	Oracle RDBMS 11gR2 x64	Oracle RDBMS 11gR2 x64
Softvér Oracle	Oracle klient 11gR2 32-bit	Oracle klient 11gR2 32-bit
Web server	Microsoft IIS na podporovanom OS	Microsoft IIS na podporovanom OS
Softvér	MS .NET Framework 3.5 MS .NET Framework 4.7.2/4.8 Acrobat Reader 9.x alebo novší	MS .NET Framework 3.5 MS .NET Framework 4.7.2 Acrobat Reader 9.x alebo novší
Internetový prehliadač	MS Edge, Mozilla Firefox, Google Chrome	MS Edge, Mozilla Firefox, Google Chrome

** Môžu byť použité ekvivalenty virtuálnych CPU.*
*** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.*
**** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.*
***** Podporované edície operačných systémov Standard, Datacenter.*

2. Požiadavky na sieťové prostredie pre CG EGOV

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps, odporúčané 1 Gpbs,
- server pripojený 1 Gpbs v DMZ, prípadne 1 x LAN 1 Gbps, 1 x Internet 100 Mbps,

  POZN: Možnosti reálneho zapojenia závisia od sieťovej infraštruktúry a použitých prvkov (firewall, proxy servera pod.) na úrade a je možné ich čiastočne prispôsobiť.

- pevná internetová adresa,
- registrované internetové DNS záznamy typu A napr. egov.domena.sk a sync.domena.sk,
- na firewalle a proxy serveri zabezpečiť smerovania dotazov z LAN a Internetu na http://egov.domena.sk prípadne https://egov.domena.sk na vnútornú adresu servera bez zmeny hlavičky s použitím host header,
- používateľské účty pre správu a implementáciu produktov,
- administrátorský prístup na server,
- na serveri s CG EGOV
  - povolený port pre aplikačný server CG EGOV,
  - povolené porty pre komunikáciu webového servera Microsoft IIS (http, https),
  - povolená komunikácia na Oracle databázový server (TCP 1521),
  - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
  - povolená komunikácia servera do siete Internet (80, 443),
  - v prípade využitia SSL zakúpený SSL certifitkát typu SHA256 od dôveryhodnej internetovej certifikačnej autority pre daný internetový DNS, prípadne iný napr. typu wildcard (*.domena.sk),
  - v prípade využívania služieb CoraInfo povolená komunikácia na https://info.corageo.sk,
- povolená komunikácia pre synchronizáciu údajov z vnútorného servera, obyčajne port TCP 81, prípadne komunikácia na http://sync.domena.sk na porte 80,
- mailové konto s povolením zasielania mailov cez SMTP mimo lokálnu doménu (zvyčajne portal@domena.sk) pre účely zasielania servisných správ zo servera CG ISS / CG Portál ISS.

PRÍLOHA Č. 4

Bezpečnostné opatrenia a iné povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášku Národného bezpečnostného úradu č. 362/2018 Z.z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrenia (ďalej len „Príloha č. 4 „)

Objednávateľ je podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej na účely tohto Dodatku len ako „**Zákon**“) prevádzkovateľom základnej služby. Táto Zmluva je podľa § 19 Zákona zmluvou na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre objednávateľa ako prevádzkovateľa základnej služby.

Účelom tejto prílohy je zabezpečiť splnenie Zákonom ustanovenej povinnosti objednávateľa ako prevádzkovateľa základnej služby mať uzatvorenú s poskytovateľom ako treťou stranou tak ako ju definuje Zákon zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona o KB počas celej doby platnosti tejto Zmluvy, ktorá priamo súvisí so zabezpečením prevádzky a využívaním informačných systémov poskytovateľa uvedených v čl. II.1 tejto Zmluvy ďalej spolu len „**Informačné systémy CG**“) pre objednávateľa ako prevádzkovateľa základnej služby.

Práva a povinnosti vyplývajúce zmluvným stranám z tejto prílohy sa vzťahujú výlučne k základnej službe poskytovanej objednávateľom ako prevádzkovateľom základnej služby a to výlučne vo vzťahu k tým licenčným a aplikačným informačným systémom, ktoré dodal poskytovateľ pre objednávateľa ako poskytovateľa základnej služby a teda pre poskytovateľom dodané Informačné systémy CG, vo vzťahu ku ktorým poskytovateľ poskytuje prevádzkovateľovi základnej služby servis a podporu v súlade s touto Zmluvou a súčasne výlučne vo vzťahu k informačným systémom poskytovateľa prostredníctvom, ktorých poskytovateľ poskytuje objednávateľovi ako prevádzkovateľovi základnej služby servis a podporu pre Informačné systémy CG (ďalej len „Ročná podpora“) a to za podmienok a spôsobom bližšie špecifikovaným v tejto Zmluve.

Pojmy aplikované v tejto prílohe sú pojmami tak ako sú definované v § 3 na účely zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

1. **Povinnosť poskytovateľa dodržiavať bezpečnostnú politiku objednávateľa ako prevádzkovateľa základnej služby a povinnosť poskytovateľa dodržiavať a prijať bezpečnostné opatrenia.**

1.1 Poskytovateľ sa zaväzuje dodržiavať platné bezpečnostné politiky objednávateľa ako prevádzkovateľa základnej služby, ktoré sú normatívne upravené v dokumentoch objednávateľa ako prevádzkovateľa základnej služby a to od momentu kedy bude s nimi poskytovateľ riadne oboznámený. Riadnym oboznámením sa s obsahom bezpečnostných politík podľa predchádzajúcej vety sa rozumie protokolárne odovzdanie dokumentov, ktoré má poskytovateľ dodržiavať.

1.2 Poskytovateľ vyhlasuje, že sa s bezpečnostnou politikou objednávateľa ako prevádzkovateľa základnej služby oboznámil a vyjadruje súhlas s bezpečnostnou politikou prevádzkovateľa základnej služby. Bezpečnostná politika objednávateľa ako prevádzkovateľa základnej služby je uvedená v Doložke č. 1 k tejto prílohe.

1.3 Poskytovateľ sa zaväzuje dodržiavať a prijať bezpečnostné opatrenia vo vzťahu k dodaným Informačným systémom CG, vo vzťahu ku ktorým poskytovateľ poskytuje prevádzkovateľovi základnej služby Ročnú podporu v súlade s ustanoveniami tejto Zmluvy a súčasne výlučne vo vzťahu k informačným systémom poskytovateľa prostredníctvom, ktorých poskytovateľ poskytuje objednávateľovi ako prevádzkovateľovi základnej služby Ročnú podporu pre Informačné systémy CG a to pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) Zákona. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

1.4 Zmluvné strany sa dohodli, že objednávateľ ako prevádzkovateľ základnej služby prehlasuje, že s výnimkou dodanej služby Ročnej podpory v termínoch stanovených prevádzkovateľom základnej služby Informačné systémy CG prevádzkuje a spravuje prevádzkovateľ základnej

služby samostatne na vlastných sieťach (serveroch) bez toho, aby k nim mal dodávateľ osobitný prístup. Pre vylúčenie pochybností sa ustanovenia tejto prílohy č. 4 a tejto Zmluvy vzťahujú len po dobu (v čase) realizácie služby Ročná podpora prostredníctvom vzdialenej správy zo strany poskytovateľa a vo vzťahu k samotnej funkčnosti dodaných Informačných systémov CG.

2. Špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma poskytovateľ a vyjadrenie súhlasu s nimi

2.1 Bezpečnostné opatrenia pre oblasť riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s Poskytovateľom ako treťou stranou:

Poskytovateľ identifikuje technické zraniteľností informačných systémov a zariadení vo vzťahu k poskytovanej Ročnej podpore najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Objednávateľovi ako prevádzkovateľovi základnej služby prostredníctvom nasledujúcich opatrení, ak sú relevantné:

a. zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
b. zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
c. využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2.2 Bezpečnostné opatrenia pre oblasť riadenia bezpečnosti sietí a informačných systémov vo vzťahu k poskytovanej Ročnej podpore:

Poskytovateľ realizuje nasledovné opatrenia, ak sú relevantné:

a. Riadenie bezpečného prístupu medzi informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu informačných systémov, ktoré sú zabezpečené segmentáciou informačných systémov.
b. Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
c. Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
d. Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
e. Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
f. Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
g. Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
h. Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.

2.3 Bezpečnostné opatrenia pre oblasť ochrany proti škodlivému kódu a pre oblasť riadenia prístupov vo vzťahu k poskytovanej Ročnej podpore realizuje poskytovateľ nasledovné opatrenia:

a. Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci Informačných systémov CG, ktoré sú nevyhnutné na plnenie zverených úloh používateľa.
b. Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
c. Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej (i) vypracovanie zásad riadenia prístupu k informáciám; (ii) riadenia prístupu používateľov;

(iii) zodpovednosti používateľov; (iv) riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; (v) prístupu k aplikáciám; (vi) monitorovania prístupu a používania informačného systému a (vii) riadenia vzdialeného prístupu.

d. Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
e. Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
f. Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
g. Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

2.4 Bezpečnostné opatrenia pre oblasť akvizície, vývoja a údržby informačných sietí a informačných systémov a pre oblasť riešenia kybernetických bezpečnostných incidentov vo vzťahu k zabezpečeniu služieb Ročnej podpory a počas povoleného času prístupu do siete objednávateľa ako prevádzkovateľa základnej služby realizuje poskytovateľ nasledovné opatrenia: Poskytovateľ najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať priamy dopad na výkon činnosti pre objednávateľa ako prevádzkovateľa základnej služby, ak sú relevantné:

a. Oboznámenie sa s postupmi prevádzkovateľa základnej služby pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči prevádzkovateľovi základnej služby.

2.5 Bezpečnostné opatrenia pre oblasť zaznamenávania udalostí a monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje poskytovateľ: opatrenia podľa § 15 Vyhlášky najmä implementuje centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb objednávateľa ako prevádzkovateľa základnej služby.

2.6 Špecifikácia a rozsah bezpečnostných opatrení vymedzených v tomto článku prílohy je dohodnutý zmluvnými stranami len rámcovo. Zmluvné strany sa zaväzujú dodatočne doplniť konkrétne bezpečnostné opatrenia, ktoré bude musieť tá-ktorá Zmluvná strana plniť, podľa záverov, ktorý vyplynú z Analýzy rizík zo strany prevádzkovateľa základnej služby, ktorá je uvedená v Doložke č. 2 k tejto prílohe, v ktorej budú popri rizikách identifikovaný aj príslušný vlastníci rizík, a teda subjekty povinné na plnenie konkrétnych bezpečnostných opatrení.

2.7 Zmluvné strany si prostredníctvom technických zástupcov dohodnú a potvrdia presné technické špecifikácie, ktoré budú vyplývať z interných bezpečnostných opatrení objednávateľa ako prevádzkovateľa základnej infraštruktúry a to na základe zrealizovanej Analýzy rizík zo strany prevádzkovateľa základnej služby, ktorá je uvedená v Doložke č. 2. Do predloženia Analýzy rizík zo strany prevádzkovateľa základnej služby, ktorá je uvedená v Doložke č. 2 nie je poskytovateľ v omeškaní s plnením opatrení špecifikovaných v tomto článku. Bezpečnostné opatrenia v súlade s týmto článkom prijíma samotný poskytovateľ v primeranom rozsahu podľa vlastného rozhodnutia, tak aby bol naplnený účel zákona č. 69/2018 Z.z.. Objednávateľ ako prevádzkovateľ základnej služby do bezpečnostných opatrení poskytovateľa nijako nezasahuje.

2.8 Objednávateľ ako prevádzkovateľ základnej služby berie na vedomie, že aplikácií bezpečnostných opatrení bude aplikovaná len na Informačné systémy CG dodané poskytovateľom a na tie časti siete, na ktoré má poskytovateľ reálny dosah.

3. Rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu objednávateľom ako prevádzkovateľom základnej služby u poskytovateľa

3.1 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený vykonávať kontrolnú činnosť a audit u poskytovateľa, a to v rozsahu a za účelom kontroly plnenia povinnosti poskytovateľa v zmysle Zákona a tejto Zmluvy.

3.2 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený vykonať kontrolnú činnosť a/alebo audit u poskytovateľa prostredníctvom poverenej osoby, ktorej identifikačné údaje je objednávateľ ako prevádzkovateľ základnej služby povinný poskytovateľovi vopred oznámiť (ďalej len „Poverená osoba“). Poverená osoba sa v čase realizácie kontrolnej činnosti a/alebo auditu u poskytovateľa musí preukázať písomným poverením vystaveným objednávateľom ako prevádzkovateľom základnej služby na jeho vykonanie. Zmluvné strany sa dohodli, že náklady na realizáciu kontrolnej činnosti a/alebo auditu u poskytovateľa tak na strane objednávateľa ako prevádzkovateľa základnej služby ako aj na strane poskytovateľa znáša v celom rozsahu objednávateľ ako prevádzkovateľ základnej služby.

3.3 Prevádzkovateľ základnej služby je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu pravidelne raz za kalendárny rok; v prípade preukázaného podozrenia z porušenia tejto Zmluvy alebo zákona; v prípade nedodržania bezpečnostných opatrení a v prípade žiadosti dozorného orgánu podľa zákona.

3.4 Prevádzkovateľ základnej služby informuje o termíne vykonania auditu alebo kontroly poskytovateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 pracovných dní pred vykonaním auditu alebo kontroly. Poskytovateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 pracovných dní odo dňa zaslania oznámenia. Pokiaľ poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.

3.5 Prevádzkovateľ základnej služby je oprávnený vykonávať audit u poskytovateľa nasledovne, pričom zmluvné strany majú pri výkone kontrolných činností a auditu nasledovné práva a povinnosti:

a. Prevádzkovateľ základnej služby je oprávnený vykonať u poskytovateľa audit zameraný na overenie plnenia povinností poskytovateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia poskytovateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u poskytovateľa pre plnenie cieľov tejto Zmluvy.
b. Prípadné nedostatky zistené auditom je poskytovateľ povinný odstrániť bez zbytočného odkladu.
c. Prevádzkovateľ základnej služby môže audit u poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v prípade ak objednávateľ realizuje audit prostredníctvom tretej osoby, tak je táto tretia osoba pred začatím realizácie auditu povinná uzatvoriť poskytovateľom dohodu o mlčanlivosti tzv. NDA, následne práva a povinnosti objednávateľa ako prevádzkovateľa základnej služby pri výkone auditu realizuje objednávateľom ako prevádzkovateľom základnej služby poverená tretia osoba.
d. Poskytovateľ je povinný pri audite spolupracovať s objednávateľom ako prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy vo vzťahu k dodaným Informačným systémom CG a výkonu Ročnej podpory. Objednávateľ ako prevádzkovateľ základnej služby je povinný minimálne 7 pracovných dní pred samotným auditom zaslať poskytovateľovi predmet auditu s menovitým zoznam tém a oblastí v rozsahu ním dodaným Informačných systémov CG, ktorých sa audit bude týkať.
e. Objednávateľ ako prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom poskytovateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy za prítomnosti osoby poverenej poskytovateľom, na ktorú sa sťahuje bod c) tohto článku.
f. V rámci auditu je poskytovateľ povinný preukázať objednávateľovi ako prevádzkovateľovi základnej služby súlad jeho postupov s touto Zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, záväzok a poučenie svojich zamestnancov, o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.

g. Ak poskytovateľ, napriek splneniu podmienky podľa pís. c) a d) tohto článku objednávateľom ako prevádzkovateľom základnej služby, neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, to neplatí ak možnosť realizácie auditu oznámil poskytovateľ objednávateľovi ako prevádzkovateľovi základnej služby v náhradnom termíne a tento termín prevádzkovateľ základnej služby odmietol akceptovať.
h. Prevádzkovateľ základnej služby, resp. ním poverená tretia osoba je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.
i. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny poskytovateľa týkajúce sa uvedených priestorov na úseku BOZP a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO"), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal poskytovateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory poskytovateľa.

3.6 Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť prevádzkovateľovi základnej služby na účely kontroly a auditu v zmysle ust. § 28 a 29 zákona.

3.7 Poskytovateľ je povinný v lehote určenej prevádzkovateľom základnej služby, nie však skôr ako v lehote 90 dní odo dňa ich oznámenia prijať opatrenia na nápravu nedostatkov zistených auditom u prevádzkovateľa základnej služby a poskytnúť potrebnú súčinnosť prevádzkovateľovi základnej služby na ich odstránenie.

4. Vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre objednávateľa ako prevádzkovateľa základnej služby namiesto poskytovateľa

4.1 Poskytovateľ je povinný dodržiavať podmienky zapojenia nového dodávateľa do poskytovania služieb tak, ako sú upravené v tejto Servisnej zmluve

4.2 Poskytovateľ je povinný vopred informovať objednávateľa ako prevádzkovateľa základnej služby o zapojení nového dodávateľa, a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom emailu na kontakt uvedeného v tejto Servisnej zmluve.

4.3 Poskytovateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb objednávateľa ako prevádzkovateľovi základnej služby nového dodávateľa bez predchádzajúceho výslovného písomného súhlasu objednávateľa ako prevádzkovateľa základnej služby.

4.4 Ak poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb objednávateľovi ako prevádzkovateľovi základnej služby nového dodávateľa, tomuto novému dodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Servisnej zmluve. Zodpovednosť voči objednávateľovi ako prevádzkovateľovi základnej služby nesie poskytovateľ, ak nový dodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

5. Povinnosti poskytovateľa informovať objednávateľa ako prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti

5.1 Objednávateľ ako prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu poskytovateľa o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie tejto Zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

5.2 Poskytovateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident týkajúci sa predmetu tejto Zmluvy a v zmysle Zákona a informovať objednávateľa ako prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.

5.3 V prípade, ak počas vykonávania Ročnej podpory poskytovateľ zaznamená kybernetický bezpečnostný incident je povinný bezodkladne informovať objednávateľa ako prevádzkovateľa základnej služby podľa bodu 5.2 tohto článku tejto Prílohy č. 4 hlásením kybernetického bezpečnostného incidentu prostredníctvom zaslania hlásenia na e-mailovú adresu uvedenú v tejto Zmluve v rozsahu nasledovných informácií:

a. <u>informácie o tom, kto hlási kybernetický bezpečnostný incident</u>:
   - identifikačné údaje dodávateľa,
   - funkcia a pracovné zaradenie osoby dodávateľa, ktorá hlási kybernetický bezpečnostný incident,
   - identifikačné údaje ďalších organizácií dotknutých kybernetickým bezpečnostným incidentom,

b. <u>informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu, ak sú dostupné a známe</u>:
   - kategória kybernetického bezpečnostného incidentu (bezpečnostný incident I. stupňa, bezpečnostný incident II. stupňa, bezpečnostný incident III. stupňa),
   - typ závažného kybernetického bezpečnostného incidentu
   - nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
   - škodlivý kód (vírus, malvér, ransomvér),
   - získavanie informácií (skenovanie site, odpočúvanie, sociálne inžinierstvo),
   - pokus o prienik do systému,
   - podozrenie na úspešný prienik do systému vrátane APT,
   - nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby),
   - neoprávnený prístup k informáciám, únik informácií, poškodenie informácií,
   - podvod (neautorizované využitie prostriedkov, porušenia autorských práv),
   - zraniteľnosť (ich existencia),
   - iné,
   - časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu
   - čas začiatku incidentu (ak je známy), čas a spôsob zistenia incidentu, informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,
   - detailný opis priebehu závažného kybernetického bezpečnostného incidentu a jeho prvotná príčina,
   - popis rozsahu škôd,
   - odhad závažnosti dopadu závažného kybernetického bezpečnostného incidentu na užívateľov základnej služby,

c. <u>informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom</u>:
   - prvotne zasiahnuté aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby),
   - informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity služby alebo činnosti, a či je zariadenie v čase podávania hlásenia v prevádzke,

d. <u>informácie o riešení závažného kybernetického bezpečnostného incidentu</u>:
   - stav riešenia závažného kybernetického bezpečnostného incidentu,
   - informácia o vykonaní nápravných opatrení smerujúcich k riešeniu hláseného závažného kybernetického bezpečnostného incidentu,
   - opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,

- popis možných negatívnych dopadov, opatrení a možných dôsledkov závažného kybernetického bezpečnostného incidentu,
- výsledok opatrení,
- dátum a čas realizácie opatrení.

5.4 Poskytovateľ je povinný na vyžiadanie nahlásiť objednávateľovi ako prevádzkovateľovi základnej služby ďalšie informácie požadované objednávateľom na plnenie jeho povinnosti vyplývajúcich zo Zákona, najmä je povinný poskytnúť objednávateľovi ako prevádzkovateľovi základnej služby:

a. informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované prevádzkovateľom základnej služby alebo Národným bezpečnostným úradom a ústredným orgánom od prevádzkovateľa základnej služby za účelom splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm. c) Zákona,
b. informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
c. informácie potrebné na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods.6 písm. e) Zákona oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,
d. informácie v potrebnom rozsahu na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 27 ods.10 Zákona.

5.5 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený požadovať od poskytovateľa vykonanie reaktívneho opatrenia a poskytovateľ je povinný vykonať reaktívne opatrenie v prípadoch, kedy bola objednávateľovi ako prevádzkovateľovi základnej služby uložená povinnosť vykonať reaktívne opatrenie Národným bezpečnostným úradom v zmysle Zákona vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany dodávateľa a vo vzťahu informačným systémom dodávateľa prostredníctvom, ktorých dodávateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy CG.

5.6 Poskytovateľ je povinný bezodkladne objednávateľovi ako prevádzkovateľovi základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok a poskytnúť prevádzkovateľovi základnej služby všetku potrebnú súčinnosť pri splnení povinnosti objednávateľa ako prevádzkovateľa základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok pred Národným bezpečnostným úradom vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany dodávateľa a vo vzťahu informačným systémom dodávateľa prostredníctvom, ktorých dodávateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy CG.

5.7 Objednávateľ ako prevádzkovateľ základnej služby je oprávnený požadovať od poskytovateľa návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu, a to najmä v prípadoch, kedy Národný bezpečnostný úrad požaduje od prevádzkovateľa základnej služby návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany dodávateľa a vo vzťahu informačným systémom dodávateľa prostredníctvom, ktorých dodávateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy CG (ďalej aj len „ochranné opatrenie“). Ochranné opatrenie sú prijímané na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

5.8 Poskytovateľ je povinný bezodkladne objednávateľovi ako prevádzkovateľovi základnej služby predložiť navrhované ochranné opatrenie na schválenie.

5.9 V prípade, ak poskytovateľ nenavrhne ochranné opatrenie v lehote určenej objednávateľom ako prevádzkovateľom základnej služby alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je poskytovateľ povinný poskytnúť všetku potrebné súčinnosť objednávateľovi, ktorý je povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

5.10 Bez ohľadu na ustanovenia tejto prílohy, povinnosti poskytovateľa majú len podporný charakter, táto príloha nezbavuje objednávateľa ako prevádzkovateľ základnej služby plniť povinnosti v zmysle Zákona, okrem iného § 19 ods. 6 a § 24 Zákona.

6. Ostatné dojednania súvisiace s povinnosťami zmluvných strán vyplývajúcich zo Zákona a Vyhlášky

6.1 Zmluvné strany sa dohodli, že hlásenia ďalších informácií požadovaných objednávateľom ako prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo Zákona sa uskutoční prostredníctvom helpdeskového systému.

6.2 Zmluvné strany sa dohodli, že hlásenia všetkých/akýchkoľvek informácií majúcich vplyv na Zmluvu sa uskutoční prostredníctvom helpdeskového systému.

6.3 Poskytovateľ sa zaväzuje, že po ukončení zmluvného vzťahu vráti, prevedie alebo zničí všetky informácie, ku ktorým mal prístup počas trvania zmluvného vzťahu s Objednávateľom ako prevádzkovateľovi základnej služby.

6.4 Poskytovateľ prehlasuje, že Zákonom ustanovenú povinnosť po ukončení Zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné práva na používanie softvéru licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby špecifikovanú v tejto Servisnej zmluve na objednávateľa ako prevádzkovateľa základnej služby bola splnená a to samotným dodaním Informačných systémov CG.

6.5 Poskytovateľ prehlasuje, že sa zaväzuje chrániť všetky informácie poskytnuté Objednávateľom ako prevádzkovateľom základnej služby.

PRÍLOHA Č.5

zoznam subdodávateľov

**Zhotoviteľ predkladá v Prílohe č. 5 k tejto zmluve zoznam všetkých svojich subdodávateľov (identifikačné údaje a predmet subdodávky) a údaje o osobe oprávnenej konať za každého subdodávateľa v rozsahu meno, a priezvisko, adresa pobytu, dátum narodenia. Až do splnenia tejto zmluvy je zhotoviteľ povinný oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi.*

**Zhotoviteľ je oprávnený kedykoľvek počas trvania tejto Zmluvy vymeniť ktoréhokoľvek subdodávateľa, a to za predpokladu, že nový subdodávateľ spĺňa požiadavky uvedené v ust. § 41 ods.1 písm. b) zákona č. 343/2015 Z.z o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej „ZVO"), ako aj povinnosť zápisu do registra partnerov verejného sektora, ak zákon pre takéhoto subdodávateľa tento zápis vyžaduje. Najneskôr 7 dní pred prijatím subdodávky od nového subdodávateľa, alebo od uzavretia zmluvného vzťahu s novým subdodávateľom (podľa toho, ktorá udalosť nastane skôr), je Zhotoviteľ povinný oznámiť Objednávateľovi (identifikačné) údaje o novom subdodávateľovi a o osobe oprávnenej konať za nového subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia a zároveň predložiť Objednávateľovi doklady preukazujúce, že nový subdodávateľ spĺňa podmienky účasti osobného postavenia v rozsahu požadovanom ust. § 41 ods. 1 písm. b) ZVO. Až do splnenia tejto Zmluvy je zhotoviteľ povinný oznámiť Objednávateľovi akúkoľvek zmenu údajov o novom subdodávateľovi.*