evidenční číslo smlouvy ŘLP ČR, s.p.:369/2015/PS/033/D1
evidenční číslo smlouvy ERA a.s.:

3510/2020/RLPCR

Řízení letového provozu
České republiky

Dodatek č. 1 k Servisní smlouvě na poskytování servisní podpory systémů P3D

uzavřené podle § 1746 odst. 2 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „**občanský zákoník**“)

(dále jen „**dodatek**“)

1. Smluvní strany

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)
se sídlem: Navigační 787, 252 61 Jeneč
zastoupený: Mgr. Petrem Fajtlem, výkonným ředitelem Útvaru provozního
IČO: 497 10 371
DIČ: CZ699004742
bankovní spojení: ČSOB Praha 5, č. účtu 88153/0300
SWIFT kód: CEKOCZPP
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze v oddíle A, vložce 10771

(dále jen „**ŘLP ČR, s.p.**")

a

ERA a.s.
se sídlem: Průmyslová 462, 530 03 Pardubice
zastoupený: Ing. Viktorem Sotonou, MBA, generální ředitel a předseda představenstva
IČO: 609 16 427
DIČ: CZ60916427
bankovní spojení: [redacted]
zapsaný v obchodním rejstříku vedeném u Krajského soudu v Hradci Králové, v oddíle B, vložce 1141

(dále jen „**ERA a.s. “)**

(ŘLP ČR, s.p. a ERA a.s. rovněž jako „**smluvní strany**“).

2. Preambule

2.1 Smluvní strany uzavřely dne 1.3.2016 Servisní smlouvu na poskytování servisní podpory systémů P3D (číslo smlouvy ŘLP ČR, s.p.: 369/2015/PS/033) (dále jen „**smlouva**“).

2.2 Vzhledem k tomu, že ERA a.s. byla vyhodnocena jako významný dodavatel ve smyslu § 2 písm. n) vyhlášky č. 82/2018 Sb. ze dne 21. května 2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), uzavírají smluvní strany tento dodatek, kterým do smlouvy formou přílohy ke smlouvě implementují požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti.

3. Předmět dodatku

3.1 S ohledem na skutečnosti uvedené v odst. 2.2 tohoto dodatku se smluvní strany dohodly, že nedílnou součástí smlouvy se stává příloha č. 1 tohoto dodatku, která obsahuje požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti (tj. informace týkající se bezpečnostních opatření pro smluvní vztahy s významnými dodavateli).

4. Závěrečná ustanovení dodatku

4.1 Ostatní ustanovení smlouvy zůstávají v platnosti beze změn.

4.2 **Tento dodatek se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení.**

4.3 Tento dodatek nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem jeho uveřejnění v registru smluv.

4.4 Uveřejnění. ERA a.s. bere na vědomí, že ŘLP ČR, s.p. je povinen uveřejnit smlouvu a tento dodatek v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv (zákon o registru smluv) ve znění pozdějších předpisů. Při uveřejnění výše uvedených smluvních dokumentů v registru smluv budou znečitelněny zejména tyto údaje:

4.4.1. u smlouvy bude znečitelněno: bankovní spojení ERA a.s., osoba oprávněná jednat za ŘLP ČR, s. p. v čl. 1 smlouvy a na podpisové doložce, obchodní tajemství podle odst. 4.4.1.1 dodatku jména osob v odst. 14.12 smlouvy, podpisy na smlouvě, příloha č. 2 a příloha č. 3 smlouvy.

4.4.1.1 Obchodní tajemství

Podle § 504 občanského zákoníku je obchodním tajemstvím kalkulace ceny uvedená v odst. 6.1 písm. a) a v čl. 6.1 písm. b) smlouvy a kalkulace ceny uvedená v příloze č. 1 smlouvy, proto nebudou tyto informace uveřejněny, ani poskytnuty podle odst. 4.4 dodatku.

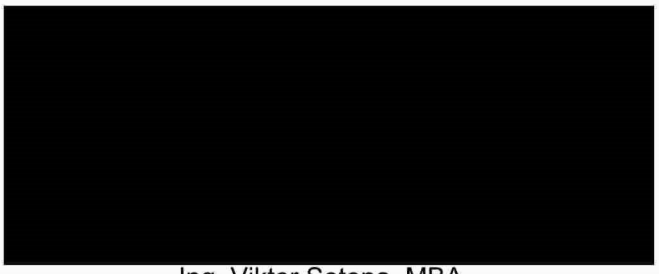
4.4.2. u tohoto dodatku bude znečitelněno: bankovní spojení ERA a.s. v čl. 1 dodatku, podpisy na dodatku.

4.5 Nedílnou součástí tohoto dodatku je následující příloha:

Příloha č. 1 dodatku (tj. příloha č. 4 smlouvy) – „Bezpečností opatření pro smluvní vztahy s významnými dodavateli dle přílohy č. 7 vyhlášky č. 82/2018 Sb. bezpečnostních opatřeních,

kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

.....
Mgr. Petr Fajtl
výkonný ředitel
Útvar provozní
Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)



Ing. Viktor Sotona, MBA
generální ředitel a předseda představenstva
ERA a.s.

Příloha dodatku č. 1 servisní smlouvy číslo 369/2015/PS/033 na poskytování podpory systémů P3D (dále též „smlouva“) k zajištění opatření v oblasti informační a kybernetické bezpečnosti

„Smluvní zajištění opatření v oblasti informační a kybernetické bezpečnosti ve smyslu § 8, odst. 2 vyhlášky č 82/2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů“

1. Preambule

1.1 Smluvní partner bere na vědomí, že je významným dodavatelem dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti pro objednatele Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.), který je správcem informačních a komunikačních systémů kritické informační infrastruktury.

1.2 [redacted]

1.3 Smluvní partner se zavazuje dodržovat požadavky systému řízení bezpečnosti chráněných informací uvedené v této příloze smlouvy a bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

2. Definice pojmů

2.1 „Aktivem“ se rozumí souhrn informací a služeb, které jsou nezbytné pro provozování informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.2 „Bezpečnostním incidentem“ se rozumí narušení bezpečnosti informací v informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.3 „Bezpečnostním opatřením“ je úkon, jehož cílem je zajištění bezpečnosti informací v informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy, jeho dostupnosti a spolehlivosti v kybernetickém prostoru.

2.4 „Bezpečnostní politikou“ je soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.

2.5 „Bezpečnostní událostí“ taková událost, která může způsobit narušení bezpečnosti informací v informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.6 „Dodavatelem“ poskytovatel dle smlouvy, který je zároveň významný dodavatel dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti.

2.7 „Kritickou informační infrastrukturou“ prvek nebo systém prvků nezbytných pro provozování informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

3. Bezpečnost informací

3.1 Dodavatel je povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy a vést o nich bezpečnostní dokumentaci.

3.2 Východiskem pro nastavení bezpečnostních opatření jsou požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhlášky o kybernetické bezpečnosti, případně normy ČSN ISO/IEC 27001.

3.3 Provádění bezpečnostních opatření u dodavatele ověřuje objednatel postupem dle čl. 15 této přílohy nebo platným certifikátem ISO/IEC 27001, případně jiným zavedeným a platným mezinárodně uznávaným systémem řízení bezpečnosti informací u dodavatele.

3.4 Dodavatel provádí opatření k zajištění důvěrnosti označených chráněných dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy v souladu s instrukcemi předanými při jejich předání, případně požadavky čl. 13 smlouvy a bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy.

3.5 Dodavatel provádí opatření k zajištění integrity dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

3.6 Dodavatel provádí opatření k zajištění dostupnosti dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy v souladu s požadavky čl. 2 a 3 smlouvy.

4. Oprávnění užívat data, pravidla přístupu

4.1 Dodavatel odpovídá za dodržování pravidel vstupu externích subjektů do areálů a objektů objednatele definovaných v čl. 5 a Příloze č. 3 smlouvy, případně bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

4.2 Dodavatel zejména odpovídá za aktuálnost seznamu pracovníků oprávněných přistupovat do objektů a k informačním / komunikačním systémům objednatele. Při ukončení pracovně-právního vztahu nebo převedení na jinou funkci pracovníka oprávněného k přístupu je dodavatel o této skutečnosti povinen neprodleně informovat objednatele prostřednictvím kontaktních osob uvedených v Příloze č. 2 smlouvy a následně iniciovat aktualizaci seznamu dle čl. 5.9 smlouvy. Seznam oprávněných pracovníků se zasílá e-mailem kontaktní osobě objednatele uvedené v Příloze č. 2 smlouvy.

4.3 Veškerá komunikace dle tohoto článku bude probíhat elektronicky podepsanými e-mailovými zprávami. Pro podepsání e-mailové komunikace může být použita interní certifikační autorita smluvního partnera nebo ŘLP ČR, s.p.

5. Autorská a licenční práva

5.1 Autorská práva a licence k informačním/komunikačním systémům uvedeným v čl. 1.2 této přílohy dodatku smlouvy se řídí ustanovením čl. 5.1 a 14.5 smlouvy.

6. Dodržování bezpečnostní politiky objednatele

6.1 Dodavatel je povinen dodržovat odsouhlasenou verzi „Bezpečnostních pravidel pro významné dodavatele“, která mu byla objednatelem zaslána dle následujícího ustanovení (dále jen „bezpečnostní pravidla“).

6.2 Aktuální verzi bezpečnostních pravidel objednatel předloží dodavateli před podpisem dodatku smlouvy, přičemž veškeré případné změny bezpečnostních pravidel (po uzavření dodatku smlouvy) vyžadované zejména v důsledku změn právních předpisů, rozhodnutí nebo varování Národního úřadu pro kybernetickou a informační bezpečnost,

rozhodnutí dalších správních úřadů nebo plnění nápravných opatření vyplývajících ze státního dozoru, budou distribuovány elektronicky podepsanými e-mailovými zprávami manažerem kybernetické bezpečnosti objednatele kontaktní osobě dodavatele uvedené v čl. 17.6 této přílohy dodatku smlouvy.

6.3 Dodavatel po obdržení bezpečnostních pravidel potvrdí jejich přijetí objednateli a potvrdí možnost a termín jejich zapracování do interních bezpečnostních politik. V případě, že dodavatel nebude schopen některé z nových pravidel provádět, vyvolá jednání s bezpečnostním manažerem objednatele a do okamžiku odsouhlasení dalších kroků postupuje v souladu s dříve akceptovanými pravidly.

6.4 Dodavatel zajistí u všech svých pracovníků, kteří se podílejí na plnění povinností dle této přílohy dodatku resp. smlouvy, prokazatelné seznámení s akceptovanými bezpečnostními pravidly.

7. Soulad s obecně závaznými právními předpisy

7.1 Dodavatel se zavazuje poskytovat servisní podporu dle smlouvy řádným způsobem a v souladu s platnými normami a obecně závaznými právními předpisy, které se na tento druh činnosti vztahují. Veškeré škody, které vzniknou porušením těchto norem a předpisů ze strany dodavatele, jdou k tíži dodavatele.

8. Řízení změn

8.1 Dodavatel je povinen řídit rizika související s plněním dle smlouvy, včetně zbytkových rizik. Na vyžádání manažera kybernetické bezpečnosti objednatele nebo osob provádějících kontrolní činnost dle čl. 15 této přílohy dodatku smlouvy je povinen způsob řízení těchto rizik doložit.

8.2 Dodavatel bere na vědomí, že objednatel při provádění změn postupuje v souladu s § 11 vyhlášky o kybernetické bezpečnosti.

8.3 U významných změn provádí objednatel analýzu rizik v souladu s metodikou CRAMM, nástrojem RAMSES.

8.4 Dodavatel poskytne objednateli nezbytnou součinnost a bude nápomocen při řízení změn, zejména při pravidelném hodnocení rizik a kontrole zavedených bezpečnostních opatření prováděných osobami určenými objednatelem. Takovou součinnost je poskytovatel povinen zajistit i u svých poddodavatelů.

8.5 [redacted]

9. Informační povinnost

9.1 Dodavatel bezodkladně informuje objednatele prostřednictvím kontaktních údajů uvedených v čl. 17.3 této přílohy dodatku smlouvy, pokud zjistí narušení bezpečnosti informací v důsledku kybernetické bezpečnostní události nebo incidentu, které souvisí se smluvním plněním a poskytne objednateli dostatečné informace, které umožní splnění všech povinností odstranit následky takové události, vyšetřit ji a ohlásit ji Národnímu úřadu pro kybernetickou bezpečnost v souladu s požadavky vyhlášky o kybernetické bezpečnosti. Dodavatel je povinen při těchto úkonech spolupracovat a přijmout finančně přiměřené kroky, které si objednatel vyžádá.

9.2 Dodavatel prostřednictvím kontaktních údajů uvedených v čl. 17.4 průběžně a bezodkladně informuje objednatele o všech jemu známých kritických hrozbách a zranitelnostech, které by mohly mít vliv na poskytování služby dodavatele v souvislosti se smluvním plněním. Objednatel se zavazuje zachovávat důvěrnost těchto informací, pokud není vázán povinností předávat tyto informace třetím stranám dle příslušných právních předpisů.

9.3 Dodavatel prostřednictvím manažera kybernetické bezpečnosti objednatele bezodkladně informuje objednatele o významné změně ovládání dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných poskytovatelem k plnění podle smlouvy s objednatelem. Má se za to, že významnou změnou ovládání se rozumí změna ovládající osoby dle § 74 a násl. zákona č. 90/2012, Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.

9.4 Podrobnější podmínky ohlašování a klasifikace událostí jsou uvedeny v bezpečnostních pravidlech.

10. Řízení kontinuity

10.1 Dodavatel postupuje při zajišťování kontinuity v souladu s pokyny předávanými oprávněnými osobami, jejichž kontaktní údaje jsou uvedeny v Příloze č. 2 smlouvy.

11. Podmínky předávání dat

11.1 Veškeré provozní údaje, databáze, soubory, obsah logů, ostatní data a informace poskytnuté a zpracovávané v souvislosti s předmětem plnění smlouvy jsou ve výhradním vlastnictví objednatele.

11.2 Předávání dat musí probíhat tak, aby nemohly neoprávněné osoby údaje číst, kopírovat, měnit ani mazat.

11.3 Uchovávání předávaných dat na datových nosičích (mobilní, ftp server) musí být zabezpečené proti přístupu neoprávněných osob.

12. Poddodavatelé

12.1 Poskytovatel objednatele dle § 105 odst. 4 ve spojení s odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, předem písemně informuje o úmyslu využít poddodavatele, kterého neoznámil v průběhu zadávacího řízení, včetně jeho identifikace a detailů činností, které má poddodavatel provádět a zpřístupňovaných dat. Identifikační údaje poddodavatelů, kteří se po uzavření smlouvy zapojí do plnění veřejné zakázky, předmět činností, které má poddodavatel provádět a zpřístupňovaná data, je poskytovatel povinen objednateli sdělit před zahájením plnění ze strany dotyčného poddodavatele.

12.2 Pokud poskytovatel sjedná s poddodavatelem provádění činností nebo zpřístupňování dat ve smyslu této přílohy smlouvy, je povinen uzavřít s poddodavatelem smlouvu nebo jiný právní akt, jež zakládá stejná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti jako jsou stanovené v této příloze smlouvy. Jedná se zejména o poskytnutí dostatečných záruk pro provedení vhodných technických a organizačních opatření tak, aby zpracování odpovídalo požadavkům vyhlášky o kybernetické bezpečnosti.

12.3 Ve vztahu ke každému poddodavateli, poskytovatel:

12.4 vynaloží veškeré přiměřené úsilí, aby prověřil, že poddodavatel poskytuje úroveň ochrany v oblasti informační a kybernetické bezpečnosti, jež je vyžadována smlouvou;

12.5 zajistí, aby při řetězení poddodavatelů byla vzájemná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti upravena písemnou smlouvou obsahující podmínky, které nabízejí alespoň stejnou úroveň ochrany jako ty, které jsou uvedeny ve smlouvě a splňují požadavky příslušných právních předpisů vztahujících se ke smluvnímu plnění;

12.6 poskytne na vyžádání objednateli kopie vybraných částí smluv s poddodavateli (nebo obdobné podklady) relevantních pro plnění smlouvy;

12.7 zajistí v rozsahu jeho činnosti, aby každý poddodavatel plnil povinnosti vyplývající ze smlouvy, které se vztahují na ochranu v oblasti informační a kybernetické bezpečnosti prováděnou tímto poddodavatelem, jako by byl stranou této smlouvy namísto poskytovatele.

12.8 V případě, že součástí uzavírané dohody s poddodavateli či mezi poddodavateli je poskytnutí bezpečnostních pravidel, je poskytovatel povinen o této skutečnosti informovat objednatele předem. Objednatel je oprávněn do pěti pracovních dnů od doručení oznámení o nutnosti poskytnutí bezpečnostních pravidel poddodavatelům namítnout, že poskytnutí bezpečnostních pravidel poddodavatelům není nezbytně nutné nebo že poskytnutí bezpečnostních pravidel konkrétnímu poddodavateli znamená pro objednatele bezpečnostní riziko a následně poskytovateli poskytnutí těchto bezpečnostních pravidel poddodavatelům nebo konkrétnímu poddodavateli zakázat. V takovém případě musí poskytovatel prokázat nezbytnou potřebu poskytnutí těchto bezpečnostních pravidel konkrétnímu poddodavateli nebo navrhnout využití jiného poddodavatele. Jestliže objednatel tuto potřebu shledá důvodnou nebo nevyhodnotí nového poddodavatele jako bezpečnostní riziko, povolí poskytnutí těchto bezpečnostních informací konkrétnímu poddodavateli.

13. Bezpečnostní podmínky při ukončení smlouvy

13.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech.

14. Pravidla pro likvidaci dat

14.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech.

15. Kontrola

15.1 Dodavatel a všichni subdodavatelé zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s tímto dodatkem a umožní a budou nápomocni při auditech a inspekcích, jakýmkoli auditorem pověřeným objednatelem. Takovou součinnost je dodavatel povinen zajistit i u svých poddodavatelů.

15.2 Objednatel se zavazuje zachovávat důvěrnost informací, které získá od dodavatele v souvislosti s prováděnými kontrolními činnostmi dle čl. 15.1.

15.3 S přiměřeným předstihem před zahájením kontroly informuje objednatel dodavatele o této kontrole. Objednatel dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrného narušení prostor, zařízení, personálu a činnosti dodavatele. Dodavatel není povinen při provádění umožnit přístup do svých prostor pouze v případě, že:

a) osoba provádějící kontrolu nepředloží doklad totožnosti a pověření k provedení kontroly;

b) je kontrola prováděna mimo běžnou pracovní dobu, leda že kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil dodavateli, že se jedná o takový případ.

15.4 Dodavatel bere na vědomí, že objednatel provádí periodické hodnocení dodavatelů v souladu s požadavky normy ČSN ISO/IEC 9001.

16. Ustanovení o sankcích za porušení povinností

16.1 Pokud dodavatel způsobí škodu porušením povinností uvedených v tomto dodatku, případně porušením povinností uvedených v bezpečnostních pravidlech, je povinen ji na vyžádání objednatele bezodkladně nahradit (nejpozději však do 10 dnů ode dne, kdy byla výše škody dodavateli objednatelem oznámena).

16.2 Je-li újma způsobena poddodavatelem, je povinen k náhradě újmy společně s dodavatelem, a to společně a nerozdílně.

16.3 Pokud dodavatel poruší podmínky režimu vstupu a vjezdu vozidel do objektů a na pozemky objednatele uvedené v čl. 5.9 smlouvy a/nebo povinnosti uvedené v čl. 4 této přílohy dodatku smlouvy a dále upřesňované v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 10.000,- Kč (slovy: desettisíc korun českých) za každý jednotlivý případ porušení.

16.4 Pokud dodavatel poruší podmínky zabezpečení koncové pracovní stanice stanovené v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč (slovy: dvacettisíc korun českých) za každý jednotlivý případ porušení.

16.5 Pokud dodavatel poruší ohlašovací povinnost v oblasti bezpečnostních událostí / incidentů stanovenou v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 50.000,- Kč (slovy: padesáttisíc korun českých) za každý jednotlivý případ porušení.

16.6 Pokud dodavatel nezajistí v určeném termínu realizaci nápravných opatření vyplývajících ze zákaznického auditu provedeného dle podmínek popsaných v čl. 15 této přílohy dodatku smlouvy a dále upřesňované v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 50.000,- Kč (slovy: padesáttisíc korun českých) za každý jednotlivý případ porušení.

16.7 Pokud dodavatel poruší ostatní povinnosti uvedené v této příloze dodatku smlouvy, případně v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč (slovy: dvacettisíc korun českých) za každý jednotlivý případ porušení.

16.8 Objednatel je oprávněn uložit po dobu trvání smlouvy smluvní pokuty v maximální souhrnné výši 500.000,- Kč (slovy: pětsettisíc korun českých).

16.9 Zaplacením smluvní pokuty nezaniká objednateli nárok na náhradu újmy v plné výši.

16.10 Porušení povinností stanovených dodavateli v tomto dodatku, případně v bezpečnostních pravidlech a/nebo významná změna kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy může být důvodem k jednostrannému ukončení smlouvy ze strany objednatele.

17. Kontaktní údaje osob odpovědných za informační a/nebo kybernetickou bezpečnost