



Řízení letového provozu České republiky

Dodatek č. 2 k servisní smlouvě „Servisní podpora systémů AMS.2“

uzavřený 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 „**objednatel**“)

a

TRANSCON ELECTRONIC SYSTEMS, spol. s r.o.

se sídlem: Ohradské náměstí 1621/5, 150 00 Praha 5

zastoupený Ing. Zdeňkem Venkrbcem, na základě plné moci v rámci Seznamu kvalifikovaných
dodavatelů – MMR ČR

IČO: 26510634

DIČ: CZ 26510634

bankovní spojení: 

zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze v oddíle C, vložce 86718

(dále jen „**poskytovatel**“)

(objednatel a poskytovatel rovněž jako „**smluvní strany**“).

3.5.5. Původní znění odst. 2.2 smlouvy se ruší a nahrazuje za nové znění takto:

„Na základě písemného požadavku objednatele na průběžný drobný rozvoj vypracuje Poskytovatel návrh řešení daného požadavku, jenž musí obsahovat i předpokládanou časovou náročnost. Realizace požadavku je zahájena až po odsouhlasení tohoto návrhu odpovědnou kontaktní osobou Objednatele. Provedená práce bude fakturována v samostatné faktuře, výše platby bude stanovena na základě počtu odpracovaných člověkohodin. Cena za jednu člověkohodinu je stanovena ■■■■■■■■

3.6 V článku 12. smlouvy se ruší odst. 12.4 a 12.5 bez náhrady. Odstavce 12.6 – 12.9 smlouvy se přečíslovávají na odst. 12.4 – 12.7 smlouvy.

3.7 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), přičemž zmíněná příloha č. 1 tohoto dodatku tvoří přílohu č. 8 smlouvy. Kontaktní údaje manažerů kybernetické bezpečnosti předají druhé smluvní straně kontaktní osoby uvedené v 3.4 této smlouvy. Tyto kontaktní údaje/osoby mohou být čas od času měněny, nicméně každá taková změna musí být druhé smluvní straně neprodleně oznámena prostřednictvím kontaktních osob uvedených v odst. 3.4 této smlouvy. Komunikace ohledně kontaktních údajů manažera kybernetické bezpečnosti bude mezi uvedenými kontaktními osobami probíhat formou dopisu zaslaného prostřednictvím poskytovatele poštovní licence, prostřednictvím datové schránky nebo elektronicky podepsaným emailem.

3.8 Znění odstavce 3.4 smlouvy se mění takto:

„Další kontakty pro účely této smlouvy budou zaslány hlavní kontaktní osobou objednatele: ■■■■■■■■ ■■■■■■■■ hlavní kontaktní osobou poskytovatele: Seznam kontaktních osob může být čas od času měněn, nicméně každá taková změna musí být objednateli či poskytovateli neprodleně oznámena. Seznam kontaktních osob a jeho změny budou zasílány mezi kontaktními osobami objednatele a poskytovatele uvedenými výše. Komunikace mezi uvedenými kontaktními osobami bude probíhat formou dopisu zaslaného prostřednictvím poskytovatele poštovní licence, prostřednictvím datové schránky nebo elektronicky podepsaným emailem.

3.9 Znění odstavce 5.3 smlouvy se mění takto:

„Objednatel umožní zaměstnancům poskytovatele, popřípadě dalším fyzickým osobám vykonávajícím práci v jeho prospěch, vzdálený přístup a připojení k systému prostřednictvím datové sítě CADIN IP, a to na základě definovaných oprávnění. Na základě těchto oprávnění bude těmto osobám protokolárně přidělen SecureID token. Způsob aktualizace seznamu osob je uveden v odst. 4.2 přílohy č. 1 tohoto dodatku.“

3.10 Ruší se příloha č. 2 smlouvy bez náhrady - Kontaktní osoby pro nahlašování servisních požadavků.

3.11 Ruší se příloha č. 3 smlouvy bez náhrady – Pracovníci poskytovatele s možností využití vzdáleného přístupu a je nahrazena postupem uvedeným v odst. 4.2 přílohy č. 1 tohoto dodatku

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 vstupuje v platnost dnem podpisu oběma smluvními stranami a účinnosti nabývá dnem jeho uveřejnění v registru smluv.

4.4 Uveřejnění. Poskytovatel bere na vědomí, že objednatel je povinen uveřejnit smlouvu, dodatek č. 1 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 smlouvy v registru smluv budou znečitelněny tyto údaje: bankovní spojení poskytovatele na první straně smlouvy, jméno osoby jednající za objednatele ve věcech technických na první straně smlouvy, částky uvedené v odst. 2.1.1, 2.1.2, 2.1.3 a 2.1.4 smlouvy (uveřejnění podléhá pouze maximální cena v odst. 2.1 smlouvy), jména v odst. 12.5 smlouvy, příloha č. 2 smlouvy, příloha č. 3 smlouvy, podpisy na smlouvě.

Při uveřejnění dodatku č. 1 v registru smluv budou znečitelněny tyto údaje: bankovní spojení poskytovatele na první straně smlouvy, jméno osoby jednající za objednatele ve věcech technických na první straně smlouvy, částky uvedené v upraveném odst. 2.1.1, 2.1.2, 2.1.3 a 2.1.4 smlouvy (uveřejnění podléhá pouze maximální cena v odst. 2.1 smlouvy), podpisy na dodatku č. 1.

Při uveřejnění tohoto dodatku č. 2 v registru smluv bude znečitelněno: bankovní spojení poskytovatele v čl. 1 a odst. 3.1 dodatku, částky uvedené v odst. 3.5 dodatku, emaily v odst. 3.8 dodatku a podpisy na dodatku.

4.5 Nedílnou součástí tohoto dodatku je následující příloha:

Příloha č. 1 – Příloha č. 8 „Bezpečnostní opatření pro smluvní vztahy s významnými dodavateli dle přílohy č. 7 vyhlášky č. 82/2018 Sb. bezpečnostních opatření, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“

.....
Mgr. Petr Fajtl

výkonný ředitel Útvaru provozního

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)

.....
Ing. Zdeněk Venkrbec

zástupce generálního ředitele

TRANSCON ELECTRONIC SYSTEMS, spol. s r.o.

Příloha č. 1 dodatku č. 2 servisní smlouvy číslo 12/12 na servisní podporu systémů AMS.2 (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. Dodavatelem se pro účely této přílohy dodatku smlouvy rozumí společnost TRANSCON ELECTRONIC SYSTEMS, spol. s r.o. Objednatelem se pro účely této přílohy dodatku smlouvy rozumí ŘLP ČR, s.p.
- 1.2 Informačními / komunikačními systémy, k nimž se vztahuje role významného dodavatele, jsou: **AMS 3**.
- 1.3 Dodavatel se zavazuje dodržovat požadavky systému řízení bezpečnosti chráněných informací uvedené v této příloze dodatku smlouvy, smlouvě a bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.
- 1.4 Plnění dále uvedených bezpečnostních pravidel vyžaduje objednatel ve vztahu ke všem informačním / komunikačním systémům uvedeným v čl. 1.2 této přílohy dodatku smlouvy. U ostatních podporovaných systémů je dodržování bezpečnostních pravidel vyžadováno přiměřeným způsobem v souladu s nejlepší praxí informační bezpečnosti.
- 1.5 Pokud je některé z ustanovení smlouvy a jejích příloh v konfliktu s ustanoveními této přílohy dodatku smlouvy nebo bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy, postupuje dodavatel v souladu s ustanoveními později uzavřeného ujednání.

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 chráněných informací v informačních / komunikačních systémech uvedených v čl. 1.2 této přílohy dodatku smlouvy.
- 2.3 „Bezpečnostním opatřením“ je úkon, jehož cílem je zajištění bezpečnosti chráněných informací v informačních / komunikačních systémech 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 chráněných informací v informačních / komunikačních systémech uvedených v čl. 1.2 této přílohy dodatku smlouvy.
- 2.6 „Dodavatelem“ 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.
- 2.8 „Subdodavatelem“ – dodavatel, který poskytuje služby nebo výrobky dodavateli. Přitom musí jít o produkty nezbytné pro zajištění bezpečnosti informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy. Nejedná se o dodavatele typizovaného hardware a / nebo softwarového řešení (COTS).

3. Bezpečnost chráněných 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 Výchozími podmínkami 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 dodatku smlouvy 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 dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy v souladu s 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 v souladu s bezpečnostními pravidly distribuovanými v souladu s čl. 6 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 §3 smlouvy.

4. Oprávnění užívat data, pravidla přístupu

- 4.1 Dodavatel odpovídá za dodržování pravidel přístupu definovaných v čl. 6.11 smlouvy, případně bezpečnostních pravidel 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 pracovního 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 oprávněných pracovníků. Seznam oprávněných pracovníků se zasílá e-mailem příslušné kontaktní osobě objednatele uvedené v příloze č. 2 smlouvy..
- 4.3 Veškerá komunikace dle tohoto článku bude probíhat elektronicky podepsanými e-mailovými zprávami.

5. Autorská a licenční práva

- 5.1 Dodavatel odpovídá za ochranu autorských a licenčních práv v souladu s čl. 6.1 smlouvy.

6. Dodržování bezpečnostní politiky objednatele

- 6.1 Dodavatel zajistí u všech svých pracovníků, kteří se podílejí na plnění povinností dle této přílohy dodatku resp. smlouvy, prokazatelné seznámení s bezpečnostními pravidly objednatele, která budou distribuována elektronicky podepsanými e-mailovými zprávami manažerem kybernetické bezpečnosti objednatele kontaktní osobě dodavatele uvedené v čl. 17.6 této přílohy dodatku smlouvy, případně jiným způsobem popsaným ve smlouvě.

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 a všichni subdodavatelé poskytnou objednateli nezbytnou součinnost a budou nápomocni při řízení změn, zejména při pravidelném hodnocení rizik a kontrole zavedených bezpečnostních opatření prováděných osobami určenými objednatelem.
- 8.5 V případě, že dodavatel v rámci svého řešení nezbytného pro poskytování služeb dle smlouvy využívá technických nebo programových prostředků společností Huawei Technologies Co., Ltd. nebo ZTE Corporation, včetně jejich dceřiných společností, je povinen předložit manažerovi kybernetické bezpečnosti objednatele nejpozději ke dni podpisu této přílohy dodatku smlouvy analýzu rizik zpracovanou v souladu s metodikou Národního úřadu pro kybernetickou bezpečnost.

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 chráněných informací v důsledku kybernetické bezpečnostní události 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 hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných objednatelem.
- 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 tímto dodavatelem k plnění podle smlouvy s objednatelem.
- 9.4 Podrobnější podmínky ohlašování a klasifikace událostí jsou uvedeny v bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

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 chráněná 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. Subdodavatelé

- 12.1 Dodavatel může využívat služeb subdodavatelů, pokud splní povinnosti stanovené příslušnými právními předpisy, zejména vyhláškou o kybernetické bezpečnosti. Dodavatel předloží objednateli ke dni podpisu této přílohy dodatku ke smlouvě seznam využívaných subdodavatelů.
- 12.2 Dodavatel objednatele předem písemně informuje o úmyslu určit nového subdodavatele, včetně detailů činností, které má subdodavatel provádět a zpřístupňovaných dat. Pokud do 30 dnů od obdržení tohoto oznámení objednatel sdělí dodavateli písemně jakékoliv námitky (z přiměřených důvodů) k navrhovanému určení, dodavatel nesmí navrhovanému subdodavateli přidělit žádné činnosti ani zpřístupnit žádná data vážící se k plnění dle této přílohy dodatku smlouvy, s výjimkou předchozího písemného souhlasu poskytnutého objednatelem.

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

12.4 Ve vztahu ke každému subdodavateli, dodavatel:

- a) vynaloží veškeré přiměřené úsilí, aby prověřil, že subdodavatel poskytuje úroveň ochrany v oblasti informační a kybernetické bezpečnosti, jež je vyžadována smlouvou;
- b) zajistí, aby při řetězení subdodavatelů 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 v této příloze dodatku resp. ve smlouvě, a splňují požadavky vyhlášky o kybernetické bezpečnosti;
- c) poskytne na vyžádání objednateli kopie dodavatelských smluv (nebo obdobné podklady) se subdodavateli;
- d) zajistí, aby každý subdodavatel plnil povinnosti vyplývající z této přílohy dodatku smlouvy, které se vztahují na ochranu v oblasti informační a kybernetické bezpečnosti prováděnou tímto subdodavatelem, jako by byl stranou této smlouvy namísto dodavatele.

13. Bezpečnostní podmínky při ukončení smlouvy

13.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech distribuovaných podle čl. 6 této přílohy dodatku smlouvy.

14. Pravidla pro likvidaci dat

14.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech distribuovaných podle čl. 6 této přílohy dodatku smlouvy.

15. Kontrola

15.1 Dodavatel a všichni subdodavatelé zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s touto přílohou dodatku smlouvy a umožní a budou nápomocni při auditech a inspekcích, jakýmkoli auditorem pověřeným objednatel.

15.2 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.

15.3 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 této příloze dodatku smlouvy, případně porušením povinností uvedených v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, je povinen ji na vyžádání objednatel bezodkladně nahradit (nejpozději však do 10 dnů ode dne, kdy byla výše škody dodavateli objednatel oznámena).

16.2 Je-li újma způsobena subdodavatelem, 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. 6.6 smlouvy a/nebo povinnosti uvedené v čl. 4 této přílohy dodatku smlouvy a dále upřesňované v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý případ porušení.
- 16.4 Pokud dodavatel poruší podmínky zabezpečení koncové pracovní stanice stanovené v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč (slovy: dvacet tisíc korun českých) za každý jednotlivý případ porušení.
- 16.5 Pokud dodavatel poruší ohlašovací povinnost v oblasti bezpečnostních událostí / incidentů stanovenou v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 100.000,- Kč (slovy: sto tisíc 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 popsanych v čl. 15 této přílohy dodatku smlouvy a dále upřesňované v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení.
- 16.7 Zaplacením smluvní pokuty nezaniká objednateli nárok na náhradu újmy v plné výši.
- 16.8 Porušení povinností stanovených dodavateli v této příloze dodatku smlouvy, případně v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, 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.