evidenční číslo smlouvy ŘLP ČR, s.p.:314/2017/PS/033/D3
evidenční číslo smlouvy poskytovatele.:

4166/2020/RLPCR

Řízení letového provozu
České republiky

Dodatek č. 3 k servisní smlouvě na servisní podporu monitorovacích a ovládacích systémů

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: Ing. Janem Klasem, generálním ředitelem
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

ELVAC SOLUTIONS s.r.o.
se sídlem: Hasičská 930/53, 700 30 Ostrava Hrabůvka
zastoupený: Mgr. Romanem Grycem, jednatelem společnosti
IČO: 273 96 649
DIČ: CZ27396649
bankovní spojení: [redacted]

(dále jen „**poskytovatel“)**

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

2. Preambule

2.1 Smluvní strany uzavřely dne 19.12.2017 servisní smlouvu na servisní podporu monitorovacích a ovládacích systémů (číslo smlouvy ŘLP ČR, s.p.: 314/2017/PS/033), ve znění dodatku č. 1 ze dne 18.12.2018 a dodatku č. 2 ze dne 23.01.2020 (dále jen „**smlouva**“).

2.2 Vzhledem k tomu, že poskytovatel byl vyhodnocen 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), přičemž zmíněná příloha č. 1 tohoto dodatku tvoří přílohu č. 6 smlouvy.

3.2 Ruší se seznam pracovníků poskytovatele s možností využití vzdáleného přístupu, vč. doplňujícího textu uvedeného pod tabulkou, uvedený v Příloze č. 1 smlouvy a je nahrazen 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 nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem jeho uveřejnění v registru smluv.

4.4 Uveřejnění. Poskytovatel bere na vědomí, že objednatel je povinen uveřejnit 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 tohoto dodatku v registru smluv bude znečitelněno: bankovní spojení poskytovatele v čl. 1 dodatku, podpisy na dodatku, čl. 1.2 a čl. 17 přílohy č. 1 dodatku.

4.5 Nedílnou součástí tohoto dodatku je následující příloha:

Příloha č. 1 – „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)“

[redacted]

.....

Ing. Jan Klas

generální ředitel

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

[redacted]

.....

Mgr. Roman Gryc

jednatel

ELVAC SOLUTIONS s.r.o.

Příloha č. 1 dodatku č. 3 servisní smlouvy číslo 314/2017/PS/033 na poskytování servisní podpory monitorovacích a ovládacích systémů (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 Poskytovatel 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 Poskytovatel se zavazuje dodržovat požadavky systému řízení bezpečnosti chráněných informací uvedené v této příloze dodatku smlouvy a bezpečnostních pravidlech distribuovaných v souladu s čl. **Error! Reference source not found.** 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 systémech 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 „Poskytovatelem“ 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 Poskytovatel 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 poskytovatele 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 poskytovatele.

3.4 Poskytovatel 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 požadavky čl. 11 a 12.3 smlouvy, Přílohy č. 1 Dodatku č. 3 smlouvy a bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy.

3.5 Poskytovatel 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 Poskytovatel 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 4 smlouvy.

4. Oprávnění užívat data, pravidla přístupu

4.1 Poskytovatel odpovídá za dodržování pravidel vstupu externích subjektů do areálů a objektů objednatele definovaných v čl. 9 smlouvy a v bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

4.2 Poskytovatel 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 poskytovatel o této skutečnosti povinen neprodleně informovat objednatele prostřednictvím kontaktních osob pro uvedených Příloze č. 2 smlouvy a následně iniciovat aktualizaci příslušných seznamů oprávněných pracovníků. Seznam oprávněných pracovníků se zasílá e-mailem kontaktní osobě objednatele pro daný informační / komunikační systém 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 Autorská práva a licence k informačním/komunikačním systémům uvedených v čl. 1.2 této přílohy dodatku smlouvy se řídí ustanovením čl. 14.2 smlouvy.

6. Dodržování bezpečnostní politiky objednatele

6.1 Poskytovatel je povinen dodržovat „Bezpečnostní pravidla pro významné dodavatele“ objednatele ve znění poslední verze, která mu byla objednatelem oznámena dle následujícího ustanovení (dále jen **„bezpečnostní pravidla“**).

6.2 Aktuální verzi bezpečnostních pravidel objednatel poskytovateli předloží před podpisem smlouvy, přičemž veškeré případné změny bezpečnostních pravidel (po uzavření 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 poskytovatele uvedené v článku 17.5 této přílohy dodatku smlouvy.

7. Soulad s obecně závaznými právními předpisy

7.1 Poskytovatel 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 poskytovatele, jdou k tíži poskytovatele.

8. Řízení změn

8.1 Poskytovatel je povinen řídit rizika související s plněním dle smlouvy. 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 Poskytovatel 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 Poskytovatel poskytne objednateli nezbytnou součinnost a budou nápomocni 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 Poskytovatel, který 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 tohoto dodatku smlouvy, případně následně před každým nasazením takových prostředků analýzu rizik zpracovanou v souladu s metodikou Národního úřadu pro kybernetickou bezpečnost.

9. Informační povinnost

9.1 Poskytovatel 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 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. Poskytovatel je povinen při těchto úkonech spolupracovat a přijmout finančně přiměřené kroky, které si objednatel vyžádá.

9.2 Poskytovatel prostřednictvím kontaktních údajů uvedených v čl. 17 průběžně a bezodkladně informuje objednatele o všech jemu známých významných a kritických hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných objednatelem.

9.3 Poskytovatel prostřednictvím manažera kybernetické bezpečnosti objednatele bezodkladně informuje objednatele o významné změně ovládání poskytovatele 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 Pravidla pro řízení kontinuity související s předmětem plnění smlouvy jsou upravena v Příloze č. 3 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:

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

b) 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;

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

d) 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.

12.4 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 Poskytovatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech.

14. Pravidla pro likvidaci dat

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

15. Kontrola

15.1 Poskytovatel zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s touto přílohou smlouvy a umožní a bude nápomocen při auditech a inspekcích prováděných jakýmkoli auditorem pověřeným objednatelem. Takovou součinnost je poskytovatel povinen zajistit i u svých poddodavatelů.

15.2 S přiměřeným předstihem před zahájením kontroly informuje objednatel poskytovatele o této kontrole. Objednatel dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrnému narušení prostor, zařízení, personálu a činnosti poskytovatele. Poskytovatel není povinen při provádění kontroly 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, ledaže kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil poskytovateli, že se jedná o takový případ.

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

15.4 Objednatel je povinen zachovávat mlčenlivost o informacích získaných během kontroly a jejich případné zpřístupnění třetí straně je možné pouze se souhlasem poskytovatele.

16. Ustanovení o sankcích za porušení povinností

16.1 Pokud některá ze smluvních stran způsobí škodu porušením povinností uvedených v tomto dodatku, případně porušením povinností uvedených v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy smlouvy, je povinna ji na vyžádání druhé smluvní strany

bezodkladně nahradit (nejpozději však do 10 dnů ode dne, kdy byla výše škody druhé smluvní straně oznámena).

16.2 Je-li újma způsobena poddodavatelem některé ze smluvních stran, je poddodavatel povinen k náhradě újmy společně s příslušnou smluvní stranou, a to společně a nerozdílně.

16.3 Pokud poskytovatel poruší podmínky režimu vstupu a vjezdu vozidel do objektů a na pozemky objednatele uvedené v čl. 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 5.000,- Kč (slovy: pět tisíc korun českých) za každý jednotlivý případ porušení.

16.4 Pokud poskytovatel poruší podmínky zabezpečení koncové pracovní stanice stanovené v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý případ porušení.

16.5 Pokud poskytovatel poruší ohlašovací povinnost v oblasti bezpečnostních událostí / incidentů stanovenou v bezpečnostních pravidlech, je objednatel oprávněn požadovat smluvní pokutu ve výši 24.000,- Kč (slovy: dvacet čtyři tisíc korun českých) za každý jednotlivý případ porušení.

16.6 Pokud poskytovatel 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 24.000,- Kč (slovy: dvacet čtyři tisíc korun českých) za každý jednotlivý případ porušení.

16.7 Celková výše smluvních pokut dle čl. 16.3 až 16.6 nesmí přesáhnout částku 24.000,- Kč (slovy: dvacet čtyři tisíc korun českých) za jeden kalendářní rok.

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

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

16.10 Pokud objednatel poruší povinnost uvedenou v bodě 15.4, je poskytovatel oprávněn požadovat smluvní pokutu ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení.

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

[redacted]