Dodatek č. 1

ke Smlouvě podpoře, údržbě a rozvoji informačního systému

Číslo smlouvy Zhotovitele: 373/17

Smluvní strany:
Fakultní nemocnice v Motole
V Úvalu 84
150 06 Praha 5
IČO: 00064203
DIČ: CZ00064203

(dále jen "Objednatel") na straně jedné

a

ARION, spol. s r.o.
Kubánské náměstí 1391/11
11000 Praha 10
IČO: 45795576
DIČ: CZ45795576
Společnost je zapsaná v OR vedeném MS v Praze v oddílu C, vložka 11440

(dále jen "Poskytovatel") na straně druhé

Smluvní strany uzavírají tento Dodatek č. 1, kterým se doplňuje Smlouva o podpoře, údržbě a rozvoji informačního systému, uzavřené ze dne 2. 3. 2018 (dále jen "Smlouva") v oblasti zajištění kybernetické bezpečnosti informací.

Článek 1. - Úvodní ustanovení

Národní úřad pro kybernetickou bezpečnost (dále jen NÚKIB) rozhodl, že se v oblasti zdravotnické dokumentace vztahuje na Fakultní nemocnice v Motole Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen ZoKb), včetně Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen Vyhláška) v rozsahu poskytování Základní služby dle uvedeného zákona.

Účelem Dodatku č. 1 je zajistit soulad s ustanovením § 4 odst. 4 ZoKB, ve spojení s přílohou č. 7 Vyhlášky a stanovit závazné bezpečnostní opatření, která se vztahují na Poskytovatele, jehož předmětem plnění pro Objednatele je (výhradně či jako součást předmětu plnění jiné služby) údržba, rozvoj, implementace a/nebo podpora informačního systému PAC 2.0 a/nebo, který v souvislosti s plněním pro Objednatele přistupuje do informačního systému Objednatele, který spadá do bezpečnostního perimetru Objednatele a /nebo který v rámci poskytovaného plnění pro Objednatele zpracovává, a/nebo přenáší a/nebo ukládá a/nebo archivuje data a provozní údaje Objednatele a/nebo jeho klientů/pacientů a osob jim blízkých.

Informační systém PAC 2.0 spadá do bezpečnostního perimetru Fakultní nemocnice v Motole, a proto se na něj vztahují požadavky uvedené v ZoKB a Vyhlášce.

Článek 2. - Obecné požadavky

Poskytovatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

2.1 postupovat v souladu s platnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro Objednatele, jakožto správce a provozovatele informačního sytému PAC 2.0 ze ZoKB a Vyhlášky a reflektovat případné novely uvedených právních předpisů či novou právní úpravu, a to na základě písemné objednávky Objednatele;

2.2 jmenovat nejpozději do 3 dnů po uzavření Dodatku č. 1 zodpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních opatření vyplývajících z Dodatku č. 1 a související komunikace mezi Smluvními stranami (dále také jen „Kontaktní osoba"). Kontaktní osobu sdělí Poskytovatel Objednateli písemně v téže lhůtě. Případnou změnu Kontaktní osoby na straně Poskytovatele je Poskytovatel povinen Objednateli nahlásit do 5 dnů od provedení změny;

2.3 zajistit, aby Kontaktní osoba Poskytovatele nejpozději do 30 dnů od uzavření Dodatku č. 1 potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění Smlouvy za stranu Poskytovatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito Bezpečnostními opatřeními;

2.4 předmět plnění nesmí být nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se ZoKB, a které dle analýzy rizik představují vysoké riziko; případné změny plnění v souladu s předchozí větou budou uskutečněny Poskytovatelem na základě písemné objednávky Objednatele;

2.5 dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů Objednatele resp. platné řídící dokumentace Objednatele či její části, které jsou relevantní k předmětu plnění, pokud byl Poskytovatel s takovými dokumenty nebo jejich částmi prokazatelně seznámen.

2.6 zaznamenávat podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.) a informovat o nich Objednatele;

2.7 v případě potřeby Objednatele musí Poskytovatel garantovat schopnost zrekonstruovat funkcionalitu aktiva do stavu požadovaného dle Smlouvy a pokud bude mít Objednatel k dispozici konzistentní zálohy dat zajistit importy těchto dat;

2.8 realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy v součinnosti s Objednatelem a na základě schválení konkrétních bezpečnostních opatření Objednatelem;

2.9 poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje dodaného software či po jeho předání;

2.10 dodat Objednateli systémovou a provozní bezpečnostní dokumentaci nejpozději do 30 dnů od podpisu Dodatku č. 1, a to minimálně v rozsahu stanoveném Objednatelem;

2.11 pokud součástí plnění je i instalace operačního systému případně software třetích stran, v průběhu jeho instalace musí být použity nejnovější aktualizované verze těchto produktů schválené Objednatelem;

2.12 veškeré informace vyžadující vyšší míru ochrany, poskytnuté Objednatelem při poskytování plnění, musí být chráněny vůči neautorizovanému přístupu; certifikáty, přístupová hesla

nebudou uchovávány v nešifrovaném tvaru, pokud nebude mezi Smluvními stranami v konkrétním případě dohodnuto jinak;

2.13 pokud v rámci poskytovaného plnění bude Poskytovatel instalovat software nebo jeho upgrade, musí postupovat podle hardeningových bezpečnostních politik a v souladu s bezpečnostními standardy Objednatele, pokud byl s takovými dokumenty nebo jejich částmi seznámen;

2.14 v produkčním prostředí systému PAC 2.0 bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému;

2.15 před spuštěním software v produkčním prostředí systému PAC 2.0 Poskytovatel provede kontrolu souladu daného software s bezpečnostními požadavky hardeningových bezpečnostních politik a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného software s bezpečnostními požadavky hardeningových politik, pokud byl s takovými dokumenty nebo jejich částmi seznámen;

2.16 Poskytovatel může instalovat nový software nebo nové verze software pouze na základě Objednatelem předem schválených migračních postupů, pokud byl s migračními postupy prokazatelně předem seznámen.

Článek 3. - Fyzická ochrana a bezpečnost prostředí

3.1 Poskytovatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systém PAC 2.0 anebo datové nosiče (dále také jen „Pracoviště").

3.2 Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému PAC 2.0.

Článek 4. - Řízení přístupu

4.1 Poskytovatel bere na vědomí, že přístup k systému PAC 2.0 je možné povolit pouze fyzické identitě zaměstnance Poskytovatele (popřípadě jeho Poddodavatele) zaevidované v registru identit Objednatele, a to na základě požadavku Poskytovatele na přístup.

4.2 Poskytovatel bere na vědomí, že jeho zaměstnanci musí poskytnout své osobní údaje Objednateli, a to v rozsahu nutném pro zřízení přístupu, v opačném případě Objednatel není povinen přístup k systému PAC 2.0 zaměstnanci Poskytovatele povolit. Zaměstnanec Poskytovatele s přiděleným přístupem (fyzickým, logickým) k systému PAC 2.0, bere na vědomí, že dochází ke zpracování osobních údajů během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách Objednatele.

4.3 Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci Poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

4.4 Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Poskytovatele nebo Poddodavatele. Objednatel se zavazuje každému zaměstnanci Poskytovatele nebo Poddodavatele vytvořit samostatné přístupy.

4.5 Poskytovatel se zavazuje, že vzdálený přístup do systému PAC 2.0 bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

4.6 Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby

do počítačové sítě Objednatele zažádá o schválení připojení kontaktní osobu na straně Objednatele.

4.7 Poskytovatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pokud daná činnost bude při plnění předmětu Smlouvy vyžadována.

4.8 Poskytovatel se zavazuje, že nebude instalovat a používat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

4.9 Poskytovatel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury Objednatele, jsou a budou chráněny proti malware.

4.10 Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému PAC 2.0 programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému PAC 2.0 nebo nelegální získání dat a informací.

4.11 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli v systému PAC 2.0:

a) neukládali, nesdíleli, data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;

b) nestahovali, nesdíleli, neukládali, nearchivovali a/nebo neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;

c) nezasílali řetězové emaily.

4.12 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě Objednatele, měli v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.

4.13 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému PAC 2.0 chránili autentizační prostředky a údaje k systémům Objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Poskytovatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení Bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovatel či jiné osobě ze strany Objednatele.

Článek 5. - Monitorování činností

5.1 Poskytovatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v systémovém prostředí Objednatele budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Objednatele, se kterými byl Poskytovatel seznámen.

Článek 6. - Předání a převzetí plnění

6.1 Poskytovatel odpovídá za to, že systém PAC 2.0 bude vždy obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace (patche). Činnosti Poskytovatel v souladu s předchozí větou budou uskutečněny na základě písemné objednávky Objednatele.

Článek 7. - Výměna informací

7.1 Pokud je předmětem Smlouvy výměna informací mezi smluvními stranami, musí být mezi smluvními stranami uzavřena dohoda o ochraně předmětných informací, zejména při jejich výměně, uložení, archivaci a ukončení Smlouvy.

Článek 8. - Zvládání kybernetických bezpečnostních incidentů

8.1 Poskytovatel se zavazuje, že při poskytování plnění pro Objednatele stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny kybernetické bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů neprodleně po jejich detekci Objednateli, a to v souladu s odstavcem 2.5. tohoto Dodatku.

8.2 Nastavená pravidla pro zvládání kybernetických bezpečnostních incidentů musí zajišťovat získání relevantních údajů jeho evidenci v souladu s ustanovením odstavcem 8.1 tohoto Dodatku;

8.3 Poskytovatel navrhne řešení tak, aby bylo možné zvládat a detekovat kybernetické bezpečnostní události a incidenty a realizuje opatření pro zvýšení odolnosti informačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom zejména z požadavků stanovených Vyhláškou; činnosti Poskytovatele v souladu s předchozí větou budou uskutečněny na základě písemné objednávky Objednatele;

8.4 Poskytovatel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

8.5 Poskytovatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

Článek 9. - Autorství

9.1 Poskytovatel se při poskytování plnění pro Objednatele zavazuje zajistit, aby při plnění Smlouvy dodržel podmínky stanovené zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Článek 10. - Oprávnění užívat data

10.1 Poskytovatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Poskytovateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.

10.2 Poskytovatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a Vyhláškou a dalšími souvisejícími právními předpisy.

Článek 11. - Řízení změn

11.1 Objednatel v rámci řízení změn v systému PAC 2.0 přezkoumává možné dopady změn a určuje významné změny dle Vyhlášky.

11.2 Objednatel u významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí testování systému PAC 2.0 a zajistí možnost navrácení do původního stavu.

11.3 Objednatel má povinnost informovat Poskytovatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany Poskytovatele.

11.4 Poskytovatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn uvedených v odstavcem 11.3.

11.5 Poskytovatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

11.6 V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Poskytovatel Objednateli veškerou potřebnou součinnost.

Článek 12. - Řízení kontinuity činností

12.1 Objednatel má oprávnění zapojit Poskytovatel do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Poskytovatel do plánu kontinuity činností, který souvisí se systémem PAC 2.0 a souvisejících služeb a/nebo zahrnutí Poskytovatel do havarijního plánu Objednatele.

12.2 Objednatel má povinnost informovat Poskytovatele o způsobu zapojení dle odstavce 12.1.

Článek 13. - Informační povinnost Poskytovatele

13.1 Poskytovatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Poskytovatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Poskytovatel nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy.

Článek 14. - Poddodavatelé

14.1 Poskytovatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího Poddodavatele bez předchozího konkrétního nebo obecného povolení Objednatele.

14.2 Poskytovatel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění Poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto Poddodavatelů.

14.3 Poskytovatel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.

14.4 Pokud Poskytovatel využívá za účelem plnění předmětu Smlouvy Poddodavatele, musí být tomuto Poddodavateli uloženy na základě smlouvy s Poskytovatelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná tímto Dodatkem mezi Objednatelem a Poskytovatel.

14.5 Poskytovatel se zavazuje předložit Objednateli, na základě jeho písemného vyzvání, příslušnou smlouvu s Poddodavatelem, s výjimkou informací, které jsou chráněné jako obchodní tajemství; osobní údaje; informace, které jsou chráněny smlouvou o zachování mlčenlivosti a utajované informace dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

14.6 Poskytovatel má povinnost zajistit, že Poddodavatel bude v souladu s požadavky, které Objednatel ukládá na základě tohoto Dodatku Poskytovateli.

14.7 Poskytovatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z tohoto Dodatku. V případě, že dojde k nedodržení těchto požadavků ze strany Poddodavatele Poskytovatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Poskytovatele dle Smlouvy.

Článek 15. - Kontrola a audit Poskytovatele

15.1 Poskytovatel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z tohoto Dodatku, jakož i ze ZoKB a Vyhlášky, a za tímto účelem se zavazuje umožnit Objednateli provedení kontrol, včetně auditů prováděných Objednatelem či auditorem, kterého Objednatel k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.

15.2 Poskytovatel je povinen Objednateli zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet technických a organizačních opatření.

15.3 Poskytovatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.

15.4 Kontrola nebo audit mohou být provedeny v prostorách Poskytovatele nebo jeho Poddodavatele a Poskytovatel má povinnost tyto kontroly nebo audity Objednateli či Objednateli pověřené osobě umožnit, přispět k nim a poskytnout Objednateli či Objednateli pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Poskytovateli rozumně požadovat. Řádnou kontrolu nebo audit lze provést maximálně jednou (1) za dva (2) roky. Mimořádnou kontrolu nebo audit může provádět Objednatel na základě písemné objednávky.

15.5 Objednatel má povinnost písmeně oznámit Poskytovatel provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu. Součástí oznámení bude i seznam osob, které jsou pověřeni ze strany Objednatele k provedení kontroly či auditu.

15.6 Výstupem v provedené kontroly či auditu může být auditní zpráva; s jejími výsledky bude Poskytovatel seznámen a může se k nim vyjádřit.

15.7 Poskytovatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů.

15.8 Poskytovatel je povinen pravidelně provádět také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Objednatelem, a to na základě objednávky Objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá Poskytovatel Objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

Článek 16. - Ochrana důvěrných informací

16.1 Strany se zavazují zachovat mlčenlivost o veškerých informacích, osobních údajích, datech či zprávách, o nichž se dozvěděly v souvislosti s přípravou či plněním Smlouvy (dále jen „důvěrné informace"), a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí smluvních stran.

16.2 Důvěrné informace ve smyslu Smlouvy nepředstavují utajované informace klasifikované stupněm „důvěrné" ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

16.3 Strany se zavazují, že zajistí, aby se všechny osoby oprávněné zpracovávat důvěrné informace zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti i po ukončení Smlouvy.

Článek 17. - Povinnosti při ukončení Smlouvy

17.1 Po skončení Smlouvy (bez ohledu na důvod ukončení) se Poskytovatel zavazuje zajistit v součinnosti s Objednatelem ukončení činností dle Smlouvy tak, aby nedošlo u Objednatele ke vzniku škod a předešlo se bezpečnostním rizikům ve smyslu ZoKB a Vyhlášky.

17.2 Poskytovatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost při zajištění kontinuity, migrace dat, apod. v souvislosti s ukončením Smlouvy, předat Objednateli, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, maintenance a rozvojem předmětu Smlouvy na Objednatele a/nebo nového Poskytovatele a to vše dle pokynů Objednatele.

Článek 18. - Odstoupení od smlouvy v případě významné změny kontroly

18.1 Objednatel si vyhrazuje právo jednostranně odstoupit od Smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle Smlouvy.

Článek 19. - Smluvní pokuty za porušení bezpečnosti dle tohoto Dodatku

19.1 Poskytovatel je povinen uhradit Objednateli smluvní pokutu ve výši 20 000 Kč za každé porušení povinností dle tohoto Dodatku. Na smluvní pokutu dle tohoto Dodatku se použijí ustanovení o sankcích dle Smlouvy.

Článek 20. - Ustanovení společná a závěrečná

20.1 Tento Dodatek je v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení tohoto Dodatku stane neplatným či nevymahatelným, nebude to mít vliv na platnost

a vymahatelnost ostatních ustanovení tohoto Dodatku a rovněž Smlouvy. Tento Dodatek doplňuje ustanovení Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a tohoto Dodatku.

20.2 Tento Dodatek může být měněn a doplňován pouze prostřednictvím písemných průběžně číslovaných dodatků, podepsaných oběma smluvními stranami.

V Praze dne 21.9.2020

.....
Objednatel

V Praze dne 2.9.2020

.....
Poskytovatel