**DODATEK č. 2 KE SMLOUVĚ**uzavřené dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb.,

občanského zákoníku v platném znění, číslo smlouvy 00212/SRV

mezi:

**MERO ČR, a.s.**

se sídlem Kralupy nad Vltavou, Veltruská 748, PSČ 278 01

IČO: 601 93 468,

zastoupenou Ing. Jaroslavem Kociánem, předsedou představenstva a Ing. Otakarem Krejsou, místopředsedou představenstva

zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2334

(dále jen „**Objednatel**“)

a

**Corpus Solutions a.s.**

se sídlem Štětkova 1638/18, Nusle, 140 00 Praha 4

IČO: 25764616

zastoupenou Ing. Tomášem Přibylem, předsedou představenstva

zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 5936

(dále jen „**Poskytovatel**")

(Objednatel a Poskytovatel společně dále jen „**Smluvní strany**“a každý jednotlivě dále jen „**Smluvní strana**“)

Vzhledem k tomu, že:

1. Smluvní strany jsou stranami smlouvy č. 00212/SRV – Smlouvy o podpoře a údržbě bezpečnostního perimetru datové sítě ze dne 16. 10. 2017 (dále jen „**Smlouva**“);
2. Objednatel je ve smyslu § 2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZoKB**“), správcem informačního a komunikačního systému kritické informační infrastruktury s označením KII MERO 01 s pracovním názvem Informační systém pro řízení mezinárodních ropovodů (dále jen společně „**Systém**“) a jako takový je povinen plnit povinnosti stanovené ZoKB a vyhláškou 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), ve znění pozdějších předpisů (dále jen „**Vyhláška o KB**“), případně jinými právními předpisy, jež upravují oblast kybernetické bezpečnosti;
3. Poskytovatel, který na základě Smlouvy poskytuje Objednateli služby spočívající v podpoře a údržbě bezpečnostního perimetru datové sítě a s nimi související služby na hardware a software, se stal provozovatelem informačního systému kritické informační struktury ve smyslu § 2 písm. g) ve spojení s § 3 písm. c) ZoKB a zároveň je jako významný dodavatel ve smyslu § 2 písm. n) Vyhlášky o KB veden Objednatelem v evidenci významných dodavatelů, a jako takový je rovněž povinen plnit povinnosti stanovené ZoKB a Vyhláškou o KB, případně jinými právními předpisy, jež upravují oblast kybernetické bezpečnosti; a

uzavírají tento Dodatek č. 2 - Pravidla kybernetické bezpečnosti společnosti MERO ČR, a.s. (dále jen **„Dodatek č. 2**“).

1. **POVINNOSTI SMLUVNÍCH STRAN** 
   1. Objednatel, jako povinná osoba dle ZoKB, má ve smyslu § 8 Vyhlášky o KB mimo jiné povinnost:
2. stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací;
3. vést evidenci svých významných dodavatelů;
4. seznamovat své dodavatele s pravidly podle písmene a) a vyžadovat plnění těchto pravidel; a
5. v souvislosti s řízením rizik spojených s významnými dodavateli zajistit, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k Vyhlášce o KB.
   1. Poskytovatel je povinen dodržovat níže uvedená pravidla a povinnosti v oblasti kybernetické bezpečnosti vyplývající ze ZoKB a Vyhlášky o KB (dále jen „**Pravidla KB**“).
6. **BEZPEČNOST INFORMACÍ Z POHLEDU DŮVĚRNOSTI, DOSTUPNOSTI A INTEGRITY**
   1. Poskytovatel se zavazuje a je povinen v rámci služeb poskytovaných Objednateli zajistit zabezpečení všech získaných či spravovaných informací a dat souvisejících se Systémem, a to zejména z hlediska jejich dostupnosti, důvěrnosti a integrity, přijmout náležitá technická a organizační opatření pro jejich zabezpečení a ukládat tato data a informace v souladu s účelem Smlouvy. Stav zajištění dostupnosti, důvěrnosti, integrity a kybernetické bezpečnosti informací souvisejících se Systémem může být ze strany Objednatele u Poskytovatele zkontrolován v rámci předem ohlášené bezpečností kontroly a auditu (viz bod 4 níže).
   2. Poskytovatel při plnění Smlouvy nakládá s následujícími typy informací souvisejících se Systémem:

- provozní a technické údaje

- osobní údaje (přihlašovací údaje)

* 1. Při nakládání s provozními údaji je Poskytovatel povinen zajistit jejich integritu. Při nakládání s osobními údaji je Poskytovatel povinen postupovat s Obecným nařízením o zpracování osobních údajů (EU) 2016/679. Poskytovatel je povinen zajistit důvěrnost informací, které se dozvěděl/získal nebo, které mu byly poskytnuty objednatelem při plnění této smlouvy, tj. není oprávněn tyto informace zpřístupnit nebo sdělit či zveřejnit třetím osobám.

1. **OPRÁVNĚNÍ UŽÍVAT DATA**
   1. Vlastníkem informací a dat souvisejících se Systémem je Objednatel. Poskytovatel je oprávněn v rámci plnění Smlouvy tyto data a informace užívat.
   2. Poskytovatel se zavazuje a je povinen využívat všechna získaná data a informace související se Systémem od Objednatele výlučně k účelu plnění této smlouvy.
   3. Na základě žádosti Poskytovatele je možné s předchozím souhlasem garanta a manažera řídicích systémů Objednatele zřídit administrátorský účet pro Poskytovatele za účelem správy dat a informací. O udělení souhlasu garanta a manažera řídicích systémů s vytvořením nového administrátorského účtu bude vždy sepsán protokol. Podrobný proces přidělování, schvalování, kontroly a rušení administrátorských účtů je upraven v interní směrnici Objednatele, s níž byl Poskytovatel seznámen.
   4. Nakládání s informacemi a daty souvisejícími se Systémem upravuje bod 2 těchto Pravidel KB. Nakládání s informacemi a daty souvisejícími se Systémem po ukončení spolupráce s Poskytovatelem upravuje bod 11 těchto Pravidel KB.
2. **KONTROLA A AUDIT POSKYTOVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)**
   1. Poskytovatel se zavazuje a je povinen umožnit Objednateli provést 1x ročně po předchozím oznámení nejméně 14 dní předem kontrolu a audit přímo u Poskytovatele a v jeho rámci zpřístupnit Objednateli informace související s plněním Smlouvy ve smyslu normy ISO 19011:2012. Bezpečnostní kontrolu nebo audit provede Objednatel vlastními silami nebo prostřednictvím řádně pověřené třetí osoby, která bude ze strany Objednatele zavázána k mlčenlivosti o zjištěních učiněných během výkonu bezpečnostní kontroly a auditu u Poskytovatele. Rozsah kontroly a auditu je dán požadavky na Poskytovatele dle Smlouvy.
   2. Základními referenčními normami pro kontrolu bezpečnostních opatření u Poskytovatele jsou ISO/IEC 27001:2014 a ISA/IEC-62443. Má-li Poskytovatel zavedený a nezávislým certifikačním orgánem certifikovaný systém bezpečnosti informací dle normy ISO/IEC 27001:2014 (minimálně pro rozsah poskytovaných služeb), je možné k tomuto při provádění kontroly a auditu ze strany Objednatele přihlédnout a omezit se na kontrolu funkčnosti Systému. Výše uvedenou certifikací dle normy ISO/IEC 27001:2014 však nelze nahradit provedení celé bezpečnostní kontroly a auditu ze strany Objednatele.
   3. Součástí prováděné bezpečnostní kontroly a auditu musí na vyžádání Objednatele být umožnění otestování:

• procesů zvládání kybernetických bezpečnostních incidentů u Poskytovatele;

• havarijních plánů a plánů kontinuity služeb Poskytovatele; a

• bezpečnostních parametrů služeb a dodávek servisních služeb poskytovaných Poskytovatelem.

1. **ŘETĚZENÍ DODAVATELŮ A SUBDODAVATELÉ**
   1. V případě, že Poskytovatel využije v rámci dodávek servisních služeb pro Objednatele své subdodavatele, zavazuje se a je povinen smluvně zajistit, že všichni subdodavatelé budou dodržovat v plném rozsahu smluvní ujednání mezi Objednatelem a Poskytovatelem, včetně těchto Pravidel KB. Poskytovatel se dále zavazuje a je povinen zajistit, že se všichni jeho subdodavatelé zaváží zajistit bezpečnost informací a dat Objednatele souvisejících se Systémem ve stejném rozsahu jako Poskytovatel. Poskytovatel je povinen Objednateli poskytnout seznam všech svých subdodavatelů (včetně kontaktních informací), kteří se budou na dodávce servisních služeb pro Objednatele podílet. Poskytovatel se zavazuje zajistit, že jeho subdodavatelé umožní Objednateli provést kontrolu a audit dle ustanovení bodu 4 těchto Pravidel KB.
2. **BEZPEČNOSTNÍ POLITIKY SPOLEČNOSTI MERO**
   1. Objednatel přijal řadu interních směrnic, které dohromady tvoří bezpečnostní politiku Objednatele. Poskytovatel se zavazuje a je povinen seznámit se s relevantním obsahem bezpečnostních politik Objednatele týkajících se kybernetické bezpečnosti a plně je dodržovat.
   2. Objednatele j oprávněn směrnice, které dohromady tvoří bezpečnostní politiku Objednatele, dle vlastního uvážení měnit a doplňovat. Relevantní obsah změněných či doplněných bezpečnostních politik Objednatel vždy s dostatečným předstihem zašle Poskytovateli k seznámení.
   3. Poskytovatel byl s relevantním obsahem bezpečnostních politik Objednatele týkajících se kybernetické bezpečnosti seznámen při podpisu tohoto Dodatku č. 2.
3. **ŘÍZENÍ ZMĚN**
   1. Veškeré změny Smlouvy nebo těchto Pravidel KB, které budou vyvolány změnou ZoKB a Vyhlášky o KB nebo předpisy na ně navazující, je nahrazující nebo s nimi související, je Objednatel oprávněn provádět jednostranně s tím, že Poskytovatel bude o těchto změnách informován s dostatečným předstihem.
   2. Poskytovatel je povinen informovat Objednatele o potřebě provedení změn v Systému, která vyvstane při plnění Smlouvy, bezodkladně po jejím zjištění. Objednatel následně určí, které změny Systému, jež mají být provedeny, je nutno považovat za významné.
   3. U významných změn v Systému jsou Objednatel a Poskytovatel povinni ve vzájemné součinnosti:
4. dokumentovat řízení těchto změn;
5. provést analýzu rizik za účelem přezkumu možných dopadů změn na Systém a kybernetickou bezpečnost a na základě jejích výsledků rozhodnout o nutnosti provést penetrační testování nebo testování zranitelností Systému;
6. přijmout opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami na Systém;
7. aktualizovat bezpečností politiku Objednatele a bezpečnostní dokumentaci, včetně těchto Pravidel KB;
8. provést testování změn a jejich funkčních dopadů na Systém; a
9. zajistit možnost navrácení Systému do původního stavu, tj. před provedením změn.
   1. Při provedení penetračního testování nebo testování zranitelností Systému dle bodu 7.3 písm. b) těchto Pravidel KB jsou Objednatel a Poskytovatel povinni ve vzájemné součinnosti v rámci aplikační bezpečnosti zajistit trvalou ochranu aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností v rámci změn v Systému a reagovat na nedostatky zjištěné během testování.
10. **SOULAD SMLUV S OBECNĚ ZÁVAZNÝMI PRÁVNÍMI PŘEDPISY**
    1. Poskytovatel se zavazuje a je povinen ve spolupráci s Objednatelem zajistit, že Smlouva je plně v souladu s aktuálními zákonnými ustanoveními a dalšími obecně závaznými právními předpisy, které stanovují požadavky na příslušné poskytované služby Poskytovatelem dle Smlouvy.
11. **INFORMAČNÍ POVINNOSTI DODAVATELE**

Poskytovatel se zavazuje a je povinen:

* 1. **Neprodleně** informovat Objednatele o kybernetických bezpečnostních incidentech nebo jiných mimořádných událostech, které se staly v Systému nebo přímo souvisí s plněním Smlouvy, a které by mohly ve svém důsledku vést k narušení bezpečnosti informací Objednatele a/nebo k ohrožení jejich ochrany, a to následujícím způsobem:

1. Primárním komunikačním kanálem pro nahlášení kybernetického bezpečnostního incidentu („**KBI**“) je e-mail [mero.incident@mero.cz](mailto:mero.incident@mero.cz).
2. Předmět zprávy by měl obsahovat typ incidentu (např. DDoS, hacking, phishing, ransomware, atd.) pro snadnější třídění incidentů. Zpráva by tak měla obsahovat například části logů obsahující záznamy o útoku, časové známky včetně časové zóny, zdrojové a cílové IP adresy a porty. Nezbytnou součástí jsou i základní kontaktní informace, tedy jméno osoby, která KBI zasílá a jméno Dodavatele.
3. Preferovaným způsobem hlášení KBI je odeslání vyplněného formuláře, který je dostupný na webových stránkách <http://www.mero.cz/dokumenty-ke-stazeni/>. Po správném a úplném vyplnění všech položek a textových polí Dodavatel soubor zašle na výše uvedenou e-mailovou adresu.
4. V případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, je **nutné** kontaktovat Objednatele na čísle +420 724 006 539.
   1. Informovat Objednatele o způsobu řízení rizik na straně Poskytovatele, identifikovaných bezpečnostních rizicích na straně Poskytovatele a o analýze a identifikaci zbytkových rizik souvisejících s plněním Smlouvy (např. riziko = špatná konfigurace, opatření = otestování před ostrým provozem, zbytkové riziko = jaké riziko zbyde po nasazení opatření).
   2. Informovat Objednatele o jakékoli významné změně vlastnické struktury, ovládání nebo kontroly nad Poskytovatelem ve smyslu zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), v platném znění (dále jen „**ZOK**“), jakož i o jakékoli změně vlastnictví nebo kontroly zásadních aktiv a změně oprávnění nakládat s těmito aktivy, která jsou využívána Dodavatelem k poskytování služeb podle Smlouvy.
5. **PODMÍNKY BEZPEČNOSTI PŘI UKONČENÍ SMLOUVY** 
   1. Poskytovatel se zavazuje a je povinen při ukončení Smlouvy či spolupráce s Objednatelem předat Objednateli veškerou technickou, projektovou, provozní a bezpečnostní dokumentaci k jednotlivým dodávaným produktům a zařízením dle Smlouvy o dílo či službám dle Smlouvy, a to v takovém rozsahu, aby byl Objednateli umožněn kontinuální bezproblémový provoz veškerých produktů a  zařízení dodaných dle Smlouvy o dílo nebo služeb poskytnutých Poskytovatelem v rámci plnění Smlouvy, a to po přechodnou dobu až do implementace a nastavení nového řešení, příp. do zahájení poskytování služeb jiným dodavatelem na stávajícím řešení. V rámci přechodného období až do implementace a nastavení nového řešení je Poskytovatel povinen poskytovat plnění dle Smlouvy a nadále provozovat Systém, pokud Objednatel Poskytovateli nesdělí jinak, a poskytovat součinnost a know-how nasazených řešeníbudoucímu dodavateli zavádějícímu nové řešení za účelem jeho úspěšné implementace, resp. dodavateli služeb, který bude pokračovat v poskytování služeb na stávajícím řešení.
   2. Na žádost Objednatele se dále Poskytovatel zavazuje a je povinen provést migraci dat a provozních údajůze stávajících systémů do nového nastavení ve formátu a dle požadavků Objednatele, příp. jejich likvidaci dle pokynů Objednatele a bodu 13 těchto Pravidel KB.
6. **PODMÍNKY PRO ŘÍZENÍ KONTINUITY ČINNOSTÍ V SOUVISLOSTI S POSKYTOVATELEM** 
   1. Poskytovatel se zavazuje a je povinen poskytnout Objednateli nezbytnou součinnost při zpracování havarijních plánů a plánů zajištění kontinuity činností. Poskytovatel souhlasí, že bude zahrnut do řízení kontinuity činností Objednatele v souvislosti s plněním dle Smlouvy. Poskytovatel prohlašuje, že byl seznámen se zněním havarijních plánů a plánů zajištění kontinuity.
7. **PODMÍNKY PRO FORMÁT PŘEDÁNÍ DAT, PROVOZNÍCH ÚDAJŮ A INFORMACÍ** 
   1. Poskytovatel se zavazuje a je povinen předávat data, provozní údaje a informace Objednateli způsobem a ve formátu specifikovaném Objednatelem a pouze osobám určeným Objednatelem. Objednatel je zároveň oprávněn určit způsob zabezpečení předávaných dat, provozních údajů a informací v souladu s jejich bezpečnostní klasifikací. Data nesmí být v žádném případě předávánav nesystematizované podobě či strojově nečitelném formátu.
8. **LIKVIDACE DAT**
   1. Poskytovatel se zavazuje a je povinen veškerá data, provozní údaje a informace, které byly Objednatelem určeny k likvidaci, zlikvidovat v souladu s přílohou č. 4 Vyhlášky o KB, přičemž konkrétní způsob likvidace určí objednatel. Poskytovatel je povinen dokladovat provedení a způsob likvidace.
9. **ODSTOUPENÍ OD SMLOUVY** 
   1. Pokud během plnění Smlouvy mezi Objednatelem a Poskytovatelem dojde nebo došlo k jakékoli významné změně vlastnické struktury, ovládání nebo kontroly nad Poskytovatelem ve smyslu ZOK, nebo k jakékoli změně vlastnictví nebo kontroly zásadních aktiv nebo změně oprávnění nakládat s těmito aktivy, která jsou využívána Poskytovatelem k poskytování plnění podle Smlouvy, je Objednatel oprávněn jednostranně odstoupit od Smlouvy, ať už byl Objednatel o takovéto změně informován Poskytovatelem v souladu s bodem 9.3 těchto Pravidel KB, či se o ní dozvěděl z jiných zdrojů.
10. **SANKCE ZA PORUŠENÍ POVINNOSTÍ A PRAVIDEL KB**
    1. Poskytovatel je povinen Objednateli uhradit veškerou mu vzniklou škodu v souvislosti s porušením Poskytovatelích povinností dle ZoKB, Vyhlášky o KB nebo těchto Pravidel KB.
    2. Objednatel je nadto oprávněn požadovat po Poskytovateli uhrazení smluvní pokuty ve výši 50.000,- Kč za každé jednotlivé porušení jeho povinností dle ZoKB, Vyhlášky o KB nebo těchto Pravidel KB.
11. **ZÁVĚREČNÁ USTANOVENÍ**
    1. Tento Dodatek č. 2 se stává platným dnem jeho podpisu oběma Smluvními stranami a účinným dnem uveřejnění v registru smluv.
    2. Tento Dodatek č. 2 je vyhotoven ve dvou stejnopisech, z nichž každá Smluvní strana obdrží po jednom.

|  |  |  |
| --- | --- | --- |
| Za Objednatele: |  | Za Poskytovatele: |
| V Kralupech nad Vltavou dne |  | V Praze dne |
|  |  |  |
| Ing. Jaroslav Kocián, předseda představenstva | Ing. Tomáš Přibyl, předseda představenstva |
| Ing. Otakar Krejsa, místopředseda představenstva |