S212-2019

DODATEK č. 1
k Rámcové dohodě na poskytování služeb

1. SMLUVNÍ STRANY

Ústav zdravotnických informací a statistiky České republiky

Organizační složka státu

se sídlem: Palackého náměstí 4, P.O. BOX 60, 128 01 Praha 2,

IČO: 00023833,

zastoupen: prof. RNDr. Ladislavem Duškem, Ph.D., ředitelem

(dále jen „**Objednatel**")

a

SKYLAB spol. s r.o.

se sídlem/místem podnikání: Zakouřilova 16/1170, 149 00 Praha 4

IČO: 25790943, DIČ: CZ25790943

subjekt zapsaný v obchodním rejstříku vedeném Městským soudem v Praze

spisová značka oddíl C, vložka 70554

bank. spojení: FIO, č. účtu: [redacted]

jehož jménem jedná: Jiřím Pokorným, jednatel

(dále jen „**Poskytovatel**")

[redacted]

2. ÚVODNÍ USTANOVENÍ

2.1 Dne 7. 5. 2018 byla mezi Ústavem zdravotnických informací a statistiky České republiky, organizační složkou státu, IČO: 00023833, se sídlem Palackého náměstí 4, P. O. BOX 60, 128 01 Praha 2 (dále jen „**Objednatel**") a SKYLAB spol. s r.o., IČO: 25790943, se sídlem Zakouřilova 16/1170, 149 00 Praha 4 (dále jen „**Poskytovatel**"), uzavřena Rámcová dohoda na poskytování služeb, vzešlá z výběrového řízení s názvem „KCICT MZ ČR", ev. čísla Z2017-034981 (dále jen „**Rámcová dohoda**").

2.2 Není-li dále uvedeno jinak, pojmy uvedené v tomto Dodatku č. 1 mají význam, jaký je jim přiřazen v Rámcové dohodě.

2.3 Jelikož Poskytovatel je významným dodavatelem ve smyslu § 2 písm. n) a § 8 odst. 1, písm. f) a odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, ve znění pozdějších předpisů, uzavírají Smluvní strany tento Dodatek č. 1, kterým se stanoví požadavky týkající se kybernetické bezpečnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů a výše uvedené vyhlášky a rovněž se také tímto Dodatkem č. 1 mění odstavec 20.3 Rámcové dohody.

3. ZMĚNA RÁMCOVÉ DOHODY

3.1 Na základě tohoto Dodatku č. 1 se Rámcová dohoda mění tak, že:

3.1.1 do čl. 2. se za odst. 2.2.4 doplňují odst. 2.2.5 a 2.2.6 následujícího znění:

*2.2.5 bere na vědomí, že Objednatel je správcem informačních systémů kritické informační infrastruktury dle ustanovení § 3 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZKB**"), správce komunikačního systému kritické informační infrastruktury dle ustanovení § 3 písm. d) ZKB a správcem významných informačních systémů dle ustanovení § 3 písm. e) ZKB. Poskytovatel dále tímto bere na vědomí, že plnění dle této Rámcové dohody bude prováděno na aktivech systémů kritické informační infrastruktury a aktivech významných informačních systému.*

*2.2.6 bere na vědomí, že Objednatel chápe Poskytovatele jako významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1, písm. f) a odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**VKB**").*

3.1.2 do čl. 4 se za odst. 4.9 doplňuje odst. 4.10 následujícího znění:

4.10 Smluvní strany potvrzují, že rozsah zapojení Poskytovatele na zajištění bezpečnostních aktiv informačních a komunikačních systémů kritické informační infrastruktury a aktiv významných informačních systémů je určen předmětem této Rámcové dohody.

3.1.3 do čl. 10 se za odst. 10.6 doplňuje odst. 10.13 a následující odst. v následujícím znění:

10.13 Poskytovatel je povinen:

a) bezodkladně oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti bezpečnosti informací Objednatele,

b) poskytnout součinnost při realizaci auditu Poskytovatele Objednatelem dle relevantních právních předpisů o kybernetické bezpečnosti,

c) informovat Objednatele o výskytu bezpečnostních incidentů dle VKB,

d) informovat Objednatele o rizicích Plnění a jejich řízení ze strany Poskytovatele,

e) informovat Objednatele o významné změně ovládání Poskytovatele. Ovládáním se rozumí vliv ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení dle VKB.

10.14 Poskytovatel prohlašuje, že má zavedena všechna bezpečnostní opatření, procesy a technologie, které prohlásil za zavedené (odpověděl ANO) ve vzorovém dotazníku pro hodnocení úrovně kybernetické bezpečnosti Poskytovatele, který tvoří Přílohu č. 1 tohoto Dodatku č. 1 Rámcové dohody.

10.15 Poskytovatel je povinen v rozsahu plnění této Rámcové dohody naplnit všechny bezpečnostní požadavky uvedené v Příloze č. 6 této Rámcové dohody. Poskytovatel umožní Objednateli v roční periodě po dobu platnosti této Rámcové dohody a 1 rok po ukončení její platnosti provedení zákaznického auditu (kontroly):

10.15.1 jehož rozsah bude ohraničen využíváním ICT prostředků Poskytovatele pro potřeby plnění této Rámcové dohody a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Poskytovatele a

10.15.2 jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle § 5 Přílohy č. 6 této Rámcové dohody.

10.16 Poskytovatel umožní Objednateli kontrolu Přílohy č. 6 této Rámcové dohody provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Poskytovatele i vzdáleně, pokud to technické prostředky Poskytovatele umožňují.

10.17 Objednatel je oprávněn při kontrole dle Přílohy č. 6 této Rámcové dohody využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou újmu.

10.18 Poskytovatel se nad rámec ustanovení této Rámcové dohody zavazuje poskytnout Objednateli součinnost minimálně v rozsahu 10

MD (MD = člověkoden v rozsahu 8 pracovních hodin) při provádění každého zákaznického auditu ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.

10.19 Poskytovatel se dále zavazuje nedostatky zjištěné:

1) na základě provedení hodnocení rizik dle § 5 v Příloze č. 6 této Rámcové dohody;

2) v rámci zákaznického auditu dle čl. 10.15 této Rámcové dohody;

odstranit ve lhůtě určené v písemném oznámení objednatele.

10.20 odst. 10.16 až 10.19 této Rámcové dohody se neaplikují, pokud je Poskytovatel pro poskytování předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. a) až g) ZKB.

10.21 Poskytovatel se nad rámec ustanovení této Rámcové dohody také zavazuje:

10.21.1 Poskytnout na vyžádání objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků dle Přílohy č. 6 této Rámcové dohody.

10.21.2 Na požádání s Objednatelem konzultovat kdykoli v průběhu realizace plnění dle této Rámcové dohody detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků dle Přílohy č. 6 této Rámcové dohody a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.

10.21.3 Neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků dle Přílohy č. 6 této Rámcové dohody, které nastanou kdykoli v průběhu trvání této Rámcové dohody.

10.21.4 Bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků dle Přílohy č. 6 této Rámcové dohody, pokud stávající řešení přestalo být funkční a efektivní.

10.21.5 Bezodkladně informovat Objednatele o bezpečnostních incidentech, které mohou ovlivnit realizaci plnění dle této Rámcové dohody.

10.21.6 Při výkonu své činnosti včas a prokazatelně upozornit objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům dle Přílohy č. 6 této Rámcové dohody a jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo obecně závaznými právními předpisy.

3.1.4 do odst. 20.12 Rámcové dohody se za slova „ Příloha č. 5 „Oprávněné osoby a realizační tým" doplňují na další řádek slova *„Příloha č. 6 Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky)".*

3.1.5 za Přílohu č. 5 Oprávněné osoby a realizační tým se doplňuje *Příloha č. 6 Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky) následujícího znění:*

Požadavky na zajištění kybernetické bezpečnosti

(Kybernetické požadavky)

§ 3 Systém řízení bezpečnosti informací

*Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §3 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „**VKB**"), které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

a. *Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění.*

b. *Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.*

c. *Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.*

d. *Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.*

e. *Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.*

§ 4 Řízení aktiv

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §4 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

   a. *Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do 30 dnů od podpisu této smlouvy a následně na vyžádání, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.*

§ 5 Řízení rizik

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §5 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

a. *Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.*

b. *V minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:*

   i. *Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok*

   ii. *Identifikaci a hodnocení rizik s vazbou na předmět plnění*

   iii. *Realizovaná bezpečnostní opatření*

   iv. *Nepokrytá bezpečnostní rizika a návrh opatření*

   v. *Vyhodnocení bezpečnostních událostí a incidentů*

   vi. *Aktuální stav souladu Dodavatele s těmito Kybernetickými požadavky*

§ 6 Organizační bezpečnost

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §6 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

   a. *Jmenovat nejpozději do 5 dnů po uzavření této smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Stranami dohody (dále také jen „Kontaktní osoba"). Kontaktní osobu sdělí Dodavatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně Dodavatele nemá dopad na ustanovení článku 17 a Přílohu č. 5 Rámcové dohody týkající se odpovědných osob ve věcech smluvních a technických.*

   b. *Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.*

§ 8 Řízení dodavatelů

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §8 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

   a. *Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Dodavatel zavazuje doložit Objednateli do 10 dnů od podpisu příslušné Prováděcí smlouvy, na jejímž plnění se budou poddodavatelé podílet, písemné prohlášení o dodržování Kybernetických požadavků u svých poddodavatelů.*

   b. *Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této smlouvy) ve smyslu příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů*

a o volném pohybu těchto údajů a zákona č. 101/2000 Sb., o ochraně osobních údajů, v platném znění, zejména pak jeho ustanovení § 6.

§ 9 Bezpečnost lidských zdrojů

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §9 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*
    a. *Zajistit, aby Kontaktní osoba nejpozději do 30 dnů od uzavření smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Dodavatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.*
    b. *Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Dodavatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.*
    c. *V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.*
    d. *Zajistit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:*
        i. *Pro uložení a sdíleni dat a informací Objednatele využívali pouze k tomu schválené prostředky (aktiva);*
        ii. *Neukládali ani nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;*
        iii. *Nestahovali, nesdíleli, neukládali, nearchivovali ani neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo AZ;*
        iv. *Nenavštěvovali internetové stránky s eticky nevhodným obsahem;*
        v. *Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;*
        vi. *Nerealizovali pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;*
        vii. *Nepodíleli se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.*
2. *Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování osobních údajů pracovníků Dodavatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Dodavatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.*

§ 10 Řízení provozu a komunikací

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §10 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*
    a. *Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.*
    b. *Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.*
    c. *Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a AZ.*

§ 11 Řízení změn

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §11 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*
    a. *Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.*
    b. *Aktivně spolupracovat při testování významné změny.*

§12 Řízení přístupu

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §12 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*
    a. *Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.*
    b. *Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Dodavatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání účinnosti této smlouvy a 2 roky po ukončení její platnosti.*
    c. *Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).*
    d. *Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.*

e. *Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují do prostředí Objednatele.*

2. *Dodavatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Dodavatele / poddodavatele Dodavatele zaevidované v Active Directory (registr identit), a to na základě požadavku Dodavatele na přístup.*
3. *Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno principem nezbytného minima a není nárokové.*
4. *Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).*

§ 13 Akvizice, vývoj a údržba

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §13 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*
    a. *Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.*
    b. *Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:*
        i. *dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů*
        ii. *dokumentaci obsahující popis autorizačního konceptu a oprávnění*
        iii. *dokumentaci obsahující instalační a konfigurační postupy*
2. *V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Dodavatel:*
    a. *Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.*
    b. *Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit objednateli vyvíjený kód SW a výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není v této smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Dodavatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito Kybernetickými požadavky.*
    c. *Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.*
    d. *Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).*

e. *Pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.*

f. *Zajistit bezpečnost testovacího prostředí u Dodavatele a ochranu poskytnutých testovacích dat Objednatelem.*

g. *Zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.*

h. *Zajistit, že v rámci poskytovaného plnění bude dodávaný software*

   i. *v souladu s bezpečnostními politikami a standardy Objednatele*

   ii. *otestován na soulad s bezpečnostními politikami Objednatele (platí pro Dodavatele, pokud byl s takovými bezpečnostními politikami seznámen)*

i. *Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.*

j. *Předat zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu.*

k. *Zajistit řízení verzí zdrojového kódu.*

l. *Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.*

m. *Zajistit, aby distribuce zdrojových kódy obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.*

n. *Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.*

§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §14 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

   a. *Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.*

   b. *Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.*

   c. *Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.*

   d. *V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele.*

e. *Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.*

f. *Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.*

2. *Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Dodavatele, nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.*

§15 Řízení kontinuity činností

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §15 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

   a. *Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.*

   b. *Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.*

§ 16 Kontrola a audit

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §8 a §16 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Úřadu dle § 23 ZKB.*

§ 17 Fyzická bezpečnost

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §17 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

   a. *Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.*

   b. *V rozsahu předmětu plnění zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Dodavatel seznámen.*

§ 18 – 27 Bezpečnostní nástroje

1. *Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v §18 až §27 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:*

    a. *Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.*

    b. *Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.*

    c. *Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této smlouvě.*

    d. *Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Dodavatele.*

    e. *Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:*

        i. *Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.*

        ii. *Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.*

        iii. *Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.*

        iv. *Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.*

        v. *Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.*

    f. *Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.*

    g. *Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.*

    h. *Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.*

    i. *Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.*

j. *Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.*

k. *Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.*

2. *Dodavatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Dodavatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato smlouva nestanoví jinak.*

3. *Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Dodavatel seznámen.*

3.1.6 za Přílohu č. 6 Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky) se doplňuje Příloha č. 1 tohoto Dodatku č. 1 - Hodnocení úrovně kybernetické bezpečnosti poskytovatele.

3.1.7 Poskytovatel před podpisem tohoto Dodatku č. 1 přistoupí ke spolupráci s Objednatelem a provede úkony vedoucí k vyhodnocení kybernetické bezpečnosti Poskytovatele.

3.1.8 do čl. 11.8 Smluvní pokuty se po odst. 11.8.5 doplňují odst. 11.8.6 a 11.8.7 v následujícím znění:

11.8.6 v případě neposkytnutí součinnosti ze strany Poskytovatele k provedení auditu Poskytovatele dle odst. 10.15, dále odst. 10.15.1 a 10.15.2 a kontrole naplnění Kybernetických (bezpečnostních) požadavků uvedených v příloze č. 6 Rámcové dohody, má Objednatel nárok na zaplacení smluvní pokuty ve výši [redacted] Kč.

11.8.7 v případě nereagování Poskytovatele na bezpečnostní incident dle VKB nejpozději do 24 hodin od jeho identifikace, má Objednatel nárok na zaplacení smluvní pokuty ve výši [redacted] Kč.

3.1.9 do čl. 18 se za odst. 18.8 doplňuje odst. 18.9 v následujícím znění:

18.9 Objednatel je oprávněn okamžitě odstoupit od Rámcové dohody či platných uzavřených prováděcích smluv v případě neposkytnutí součinnosti Poskytovatele k provedení auditu Poskytovatele dle odst. 10.15, dále odst. 10.15.1 a 10.15.2 nebo v případě okamžitého neodstranění závadného stavu vyvolaného porušením požadavků na zajištění kybernetické bezpečnosti ze strany Poskytovatele.

11.9 Na základě tohoto Dodatku č. 1 se dále mění odst. 20.3 Rámcové dohody tak, že tento odstavec nově zní:

Veškeré změny či doplnění Rámcové dohody s výjimkou změn oprávněných osob lze činit pouze na základě písemné dohody Smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma Smluvními stranami podepsaných dodatků Rámcové dohody. Oprávněné osoby jsou Smluvní strany oprávněny kdykoli změnit, a to jednostranným prohlášením. Změna je účinná okamžikem doručení oznámení druhé Smluvní straně.

11 ZÁVĚREČNÁ USTANOVENÍ

11.13 Tento Dodatek č. 1 byl vyhotoven a stranami podepsán ve 4 stejnopisech, z nichž každá ze stran obdrží po 2 stejnopisech.

11.14 Smluvní strany prohlašují, že se důkladně seznámily s celým textem tohoto Dodatku č. 1 a nemají vůči němu žádných výhrad a že tento Dodatek č. 1 vyjadřuje skutečnou, svobodnou a vážně míněnou vůli Smluvních stran, že nebyla ujednána v tísni či za nevýhodných podmínek pro žádnou z nich.

11.15 Tento Dodatek č. 1 je platný dnem jeho podpisu oběma Smluvními stranami a účinný okamžikem jeho zveřejnění v registru smluv.

11.16 Ostatní ujednání Rámcové dohody jsou tímto Dodatkem č. 1 nedotčeny.

11.17 Nedílnou součást tohoto Dodatku č. 1 Rámcové dohody tvoří tato příloha:

Příloha č. 1 Hodnocení úrovně kybernetické bezpečnosti poskytovatele

Objednatel

V Praze dne 14 -08- 2019

[redacted]

Ústav zdravotnických informací a statistiky České republiky

prof. RNDr. Ladislav Dušek, Ph.D., ředitel

Ústav zdravotnických informací a statistiky ČR
Palackého nám. 4
128 00 Praha 2, P.O. BOX 60
(4)

Poskytovatel

V Praze dne 14 -08- 2019

[redacted]

SKYLAB spol. s r.o.

[redacted]

Jiří Pokorný, jednatel

[redacted]