**Smlouva o zajištění některých požadavků kybernetické bezpečnosti**

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**občanský zákoník**“), a podle § 8 odst. 1 písm. f) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „**VKB**“), mezi těmito stranami:

**[DOPLNÍ DODAVATEL]**

IČ: [DOPLNÍ DODAVATEL]

DIČ: [DOPLNÍ DODAVATEL]

se sídlem: [DOPLNÍ DODAVATEL]

zastoupena: [DOPLNÍ DODAVATEL]

bankovní spojení: [DOPLNÍ DODAVATEL]

číslo účtu: [DOPLNÍ DODAVATEL]

zapsána v obchodním rejstříku vedeném [DOPLNÍ DODAVATEL] soudem v [DOPLNÍ DODAVATEL], oddíl [DOPLNÍ DODAVATEL], vložka [DOPLNÍ DODAVATEL],

(dále jen „**Poskytovatel**“) na straně jedné

a

**Fakultní nemocnice Brno**

IČ: 65269705

DIČ: CZ65269705

se sídlem: Brno, Jihlavská 20, PSČ 625 00

zastoupena: MUDr. Ivem Rovným, MBA, ředitelem

bankovní spojení: Česká národní banka

číslo bankovního účtu: 71234621/0710

FN Brno je státní příspěvková organizace zřízená rozhodnutím Ministerstva zdravotnictví. Nemá zákonnou povinnost zápisu do obchodního rejstříku, je zapsána v živnostenském rejstříku vedeném Živnostenským úřadem města Brna,

(dále jen „**FN Brno**“) na straně druhé,

a to v následujícím znění:

### Účel smlouvy a úvodní ujednání

* 1. FN Brno je významným poskytovatelem zdravotních služeb na základě zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, ve znění pozdějších předpisů. FN Brno při poskytování zdravotních služeb využívá systém RIS eMedSolutions, výrobce ESZFK Egészséginformatikai Szolgáltató és Fejlesztési Központ Nonprofit Korlátolt Felelősségű Társaság (ESZFK Nonprofit Kft.), 1097 Budapest, Könyves Kálmán körút 11. B. ép. 1. em., Maďarsko (dále jen „**Systém**“).
	2. Tato smlouva o zajištění některých požadavků kybernetické bezpečnosti je uzavřena v rámci zadávacího řízení na veřejnou zakázku s názvem „**Zajištění podpory systému RIS** **eMedSolution III**“ (dále jen „**Veřejná zakázka**“). Na základě tohoto zadávacího řízení FN Brno uzavřela s Poskytovatelem rovněž smlouvu, jejímž předmětem je mimo jiné poskytování služeb k Systému (dále jen „**Smlouva o poskytování služeb**“).
	3. Poskytovatel (dodavatel) bere na vědomí, že:
		1. FN Brno je dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**ZKB**“), provozovatelem základní služby a identifikuje Systém jako technické aktivum dle § 2 písm. k) VKB významné z hlediska kybernetické bezpečnosti;
		2. s ohledem na povinnosti sjednané Smlouvou o poskytování služeb je Poskytovatel v postavení významného dodavatele ve smyslu § 2 písm. n) VKB.
	4. FN Brno za účelem plnění svých povinností podle ZKB a VKB stanovila pravidla pro dodavatele dle § 8 odst. 1 písm. a) VKB, která jsou přílohou č. 1 této smlouvy a ve kterých má Poskytovatel postavení dodavatele (dále jen „**Pravidla pro dodavatele**“).
	5. Účelem této smlouvy je ve vztahu ke Smlouvě o poskytování služeb naplnění povinnosti FN Brno upravené v § 8 odst. 1 písm. f) VKB.
	6. Smluvní strany shodně prohlašují, že mají zájem zajistit provozování Systému za podmínek vysoké úrovně kybernetické bezpečnosti a postupovat při tom v souladu se ZKB a VKB. Smluvní strany se dohodly, že si za tím účelem budou poskytovat veškerou nezbytnou součinnost a uplatňovat postupy *best practices* v oblasti informační a kybernetické bezpečnosti.

# Předmět smlouvy

* 1. FN Brno je povinna **do 1 měsíce** od nabytí účinnosti této smlouvy Poskytovateli poskytnout nebo zpřístupnit údaje podle § 8 odst. 3 VKB v rozsahu, ve kterém nejsou součástí této smlouvy, a poskytnout nebo zpřístupnit bezpečnostní politiky FN Brno, kterými se rozumí dokumenty FN Brno zpracované za účelem naplnění požadavků VKB a uvedené v příloze č. 5 VKB jakožto bezpečnostní politiky. Poskytovatel bere na vědomí, že FN Brno považuje veškeré informace poskytnuté nebo zpřístupněné podle věty předchozí za důvěrné.
	2. Okamžikem splnění povinnosti FN Brno podle odst. II.1 této smlouvy se Poskytovatel považuje za řádně informovaného dle § 8 odst. 1 písm. c) VKB o tom, že je veden v evidenci významných dodavatelů FN Brno. **Smluvní strany jsou počínaje týmž okamžikem povinny při plnění Smlouvy o poskytování služeb postupovat podle Pravidel pro dodavatele a plnit povinnosti pro ně z Pravidel pro dodavatele vyplývající.** **Odměna za plnění povinností vyplývajících z této smlouvy a z Pravidel pro dodavatele je zahrnuta v odměnách sjednaných ve Smlouvě o poskytování služeb, ledaže z Pravidel pro dodavatele vyplývá něco jiného.**
	3. V případě rozporu mezi touto smlouvou a Pravidly pro dodavatele, má přednost tato smlouva. V případě rozporu mezi touto smlouvou a Smlouvou o poskytování služeb má přednost Smlouva o poskytování služeb.

# Bezpečnost informací

* 1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:
		1. si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou poskytující stranou považovány za důvěrné (dále jen „**Důvěrné informace**“);
		2. mohou jejich zaměstnanci a osoby v obdobném postavení, zejména osoby jednající z jejich pověření, získat vědomou činností druhé strany nebo i jejím opomenutím přístup k Důvěrným informacím druhé strany.
	2. Za Důvěrné informace se vždy považují:
		1. veškeré osobní údaje;
		2. informace, které jako důvěrné smluvní strana výslovně označí;
		3. veškeré informace související se zabezpečením Důvěrných informací;
		4. veškeré informace související s provozem a zabezpečením zdravotnických prostředků, přístrojů, počítačových programů a dalších systémů zpracovávajících Důvěrné informace; a
		5. veškeré informace související s provozem a zabezpečením počítačových sítí a informační a komunikační infrastruktury FN Brno.
	3. Smluvní strana, která přijala Důvěrné informace nebo které byly Důvěrné informace z jakéhokoli důvodu zpřístupněny, je povinna s odbornou péčí zachovávat jejich důvěrnost a k ochraně jejich důvěrnosti vyvíjet alespoň takové úsilí, jako by se jednalo o její vlastní důvěrné informace.
	4. Smluvní strany se zavazují, že žádná z nich Důvěrné informace nezpřístupní třetí osobě, nezveřejní ani je neužije v rozporu s účelem této smlouvy, a to ani pro svůj vlastní prospěch. Za třetí osoby podle věty první se nepovažují zaměstnanci FN Brno. Za třetí osoby podle věty první se nepovažují ani osoby, které jsou Poskytovatelem pověřeny k poskytování plnění dle této smlouvy nebo dle Smluv. Poskytovatel je však povinen tyto osoby zavázat k mlčenlivosti, zajišťování bezpečnosti informací a ochraně osobních údajů ve stejném rozsahu a za stejných podmínek, jako je k tomu sám zavázán podle této smlouvy. Poskytovatel je na písemnou výzvu FN Brno povinen FN Brno písemně prokázat existenci právního vztahu se třetí osobou splňujícího podmínky věty předchozí, a to do 5 pracovních dnů od doručení takové písemné výzvy a s uvedením zaměstnavatele takové třetí osoby, je-li to relevantní, a dále jejího jména, příjmení, pracovního zařazení, e-mailu a telefonního čísla. Poskytovatel je na písemnou výzvu FN Brno povinen FN Brno předložit seznam svých zaměstnanců podílejících se na plnění této smlouvy nebo Smluv s uvedením jména, příjmení, pracovního zařazení, e-mailu a telefonního čísla, kteří se podílejí na plnění této smlouvy, a to do 5 pracovních dnů od doručení takové písemné výzvy.
	5. Smluvní strany se zavazují poučit veškeré osoby, které se na jejich straně podílejí nebo budou podílet na plnění této smlouvy, o povinnosti zachovávat mlčenlivost a chránit Důvěrné informace podle této smlouvy a právních předpisů.
	6. V případě, že se strana této smlouvy dozvěděla, že došlo k narušení bezpečnosti Důvěrných informací druhé strany nebo je bezpečnost Důvěrných informací druhé strany vážně ohrožena, je povinna o takové skutečnosti druhou stranu bez zbytečného odkladu písemně uvědomit a přijmout veškerá smysluplná opatření na ochranu takových Důvěrných informací.
	7. Žádným ustanovením této smlouvy nejsou dotčeny povinnosti FN Brno vyplývající z právních předpisů, zejména ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ze zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.

### Závěrečná ujednání

* 1. Tato smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, v platném znění. Tato smlouva se uzavírá na dobu určitou, a to do skončení účinnosti Smlouvy o Software, a to bez ohledu na důvod, pro který byla Smlouva o Software ukončena.
	2. FN Brno je oprávněna tuto smlouvu kdykoli vypovědět, a to i bez udání důvodu. Výpovědní doba je 6 měsíců a počíná běžet prvním dnem kalendářního měsíce následujícího po kalendářním měsíci, ve kterém byla výpověď doručena Poskytovateli. Poskytovatel není oprávněn tuto smlouvu vypovědět.
	3. Ukončením účinnosti této smlouvy z jakéhokoli důvodu nejsou dotčena ujednání této smlouvy týkající se mlčenlivosti, nároků z odpovědnosti za újmu a nároky ze smluvních pokut, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po skončení účinnosti této smlouvy.
	4. Osoby podepisující tuto smlouvu jménem Poskytovatele prohlašují, že podle stanov společnosti, společenské smlouvy nebo jiného obdobného organizačního předpisu jsou oprávněny tuto smlouvu podepsat a k platnosti této smlouvy není třeba podpisu jiné osoby.
	5. Jakékoliv změny či doplňky této smlouvy lze činit pouze formou písemných číslovaných dodatků podepsaných oběma smluvními stranami. Odstoupení nebo výpověď této smlouvy lze provést pouze písemnou formou.
	6. Tato smlouva je sepsána ve dvou vyhotoveních stejné platnosti a závaznosti, přičemž každá smluvní strana obdrží jedno vyhotovení. Pokud je tato smlouva podepsána uznávaným elektronickým podpisem, obdrží každá smluvní strana její vyhotovení elektronicky podepsané oběma smluvními stranami.
	7. Smluvní strany prohlašují, že se důkladně seznámily s obsahem této smlouvy, kterému zcela rozumí a plně vyjadřuje jejich svobodnou a vážnou vůli.

 V [DOPLNÍ DODAVATEL] dne V Brně dne

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Za Poskytovatele za FN Brno

 **[DOPLNÍ DODAVATEL] Fakultní nemocnice Brno**

[DOPLNÍ DODAVATEL] MUDr. Ivo Rovný, MBA, ředitel

Příloha č. 1

PRAVIDLA PRO DODAVATELE

Tento dokument stanovuje na základě § 8 odst. 1 písm. a) a f) VKB ve spojení s přílohou č. 7 VKB závazná pravidla a bezpečnostní opatření zohledňující požadavky systému řízení bezpečnosti informací (dále také jen „***Pravidla***“), která se vztahují na dodavatele, kteří pro FN Brno (výhradně či jako součást předmětu plnění) dodávají, vyvíjí, implementují a/nebo provádějí servis software či hardware (dále také jen „***SW***“ či „***HW***“), který je uveden ve smlouvě, k níž jsou tato Pravidla připojena (dále také „***Systém***“) v souladu se ZKB a/nebo kteří v rámci poskytovaného plnění pro FN Brno zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo uchovávají informace, data a/nebo provozní údaje FN Brno, a/nebo poskytují FN Brno jiná plnění, která jsou významná z hlediska bezpečnosti Systému.

**Není-li dále výslovně uvedeno jinak, rozumí se v těchto Pravidlech pod pojmem „smlouva“ Smlouva o poskytování Služeb. Pod pojmem „zadávací dokumentace“ se rozumí zadávací dokumentace v zadávacím řízení na Veřejnou zakázku. V případě pochybností musí být ustanovení těchto Pravidel vykládána v souladu se smlouvou, ZKB, VKB a s účelem sledovaným zadávací dokumentací a těmito Pravidly.**

Bezpečnostními politikami se rozumí dokumenty FN Brno zpracované FN Brno za účelem naplnění požadavků VKB a uvedené v příloze č. 5 VKB jako bezpečnostní politiky. Dokumentací systému řízení bezpečnosti informací FN Brno se rozumí bezpečnostní politiky podle přílohy č. 5 VKB zpracované za účelem naplnění požadavků VKB dle § 30 VKB. **Ustanovení těchto Pravidel týkající se dokumentace systému řízení bezpečnosti informací FN Brno je dodavatel povinen dodržovat počínaje okamžikem, kdy byl s touto dokumentací seznámen, a pouze v rozsahu, ve kterém byl s touto dokumentací seznámen.**

Účelem těchto Pravidel je dosažení FN Brno stanovené úrovně kybernetické bezpečnosti a bezpečnosti informací v souladu s požadavky ZKB, VKB a dokumentace systému řízení bezpečnosti informací FN Brno.

Není-li dále uvedeno jinak, rozumí se pojmy užívanými v tomto dokumentu pojmy ve smyslu ZKB, VKB, nebo dokumentace systému řízení bezpečnosti informací ve FN Brno, se kterou byl dodavatel seznámen.

Pro účely těchto Pravidel se povinnosti dodavatele stanovená těmito Pravidly považují za bezpečnostní opatření.

Dodavatel je povinen poskytovat plnění dle smlouvy v souladu se všemi právními předpisy upravujícími kybernetickou bezpečnost ve FN Brno a v souladu s vnitřními předpisy FN Brno, se kterými byl FN Brno seznámen, resp. tak, aby se dodavatel vyvaroval jakékoliv činnosti, jež by mohla být označena za porušení uvedených právních předpisů nebo interních předpisů FN Brno, se kterými byl FN Brno seznámen. Pro účely těchto Pravidel platí, že veškeré povinnosti dodavatele, směřující k dosažení FN Brno stanovené úrovně kybernetické bezpečnosti a bezpečnosti informací v souladu s požadavky ZKB, VKB a dokumentace systému řízení bezpečnosti informací FN Brno, se vztahují výhradně k předmětu plnění sjednanému ve smlouvě, ledaže je výslovně stanoveno jinak.

**DODAVATEL JE PŘI POSKYTOVÁNÍ PLNĚNÍ PRO FN BRNO POVINEN PLNIT NÁSLEDUJÍCÍ POVINNOSTI:**

1. postupovat v souladu s platnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími ze ZKB a VKB, a reflektovat případné novely uvedených právních předpisů či novou právní úpravu.
2. dodavatel je povinen zachovat bezpečnost informací a dat obsažených v Systému, nebo v jiných informačních systémech, které jsou plněním této smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Plnění dle této smlouvy je dodavatel povinen poskytovat tak, aby důvěrnost, dostupnost a integrita informací a dat dle předchozí věty nebyla porušena, ohrožena, ani omezena v souladu s požadavky dokumentace systému řízení bezpečnosti informací ve FN Brno. Dodavatel prohlašuje, že si je vědom všech povinností, které je povinen z hlediska zachování bezpečnosti informací ve FN Brno dodržovat. Je-li k plnění dle této smlouvy nezbytné důvěrnost, dostupnost či integritu informací nebo dat omezit, ohrozit nebo porušit, může tak dodavatel učinit pouze po předchozím souhlasu FN Brno a jen v rozsahu FN Brno předem odsouhlaseném.
3. dodavatel je povinen FN Brno písemně informovat o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním této smlouvy, a to bez zbytečného odkladu, nejpozději do 90 dnů od nabytí účinnosti této smlouvy. Dodavatel je povinen zejména identifikovat jednotlivá konkrétní rizika spojená s plněním dle této smlouvy, jednotlivá konkrétní opatření k jejich eliminaci a zbytková rizika, která není možné přijatými opatřeními eliminovat. Dodavatel je povinen řídit rizika související s plněním této smlouvy po celou dobu účinnosti smlouvy a na žádost FN Brno způsob řízení rizik FN Brno prokázat. FN Brno je oprávněna řízení rizik dodavatelem kontrolovat a dodavatel je povinen k tomu FN Brno poskytnout nejvyšší možnou součinnost. FN Brno je oprávněna provádět kontrolu způsobu řízení rizik dodavatelem pouze v takovém rozsahu, aby tím nepřiměřeně nezasahovala do plnění dle této smlouvy, neohrozila důvěrnost, dostupnost a integritu dat dodavatele a nezvyšovala náklady na straně dodavatele.
4. smluvní strany jmenují a druhé smluvní straně sdělí nejpozději do 10 pracovních dnů od nabytí účinnosti těchto Pravidel zodpovědné kontaktní osoby pro potřeby zajištění plnění bezpečnostních opatření a související komunikace mezi smluvními stranami (dále také jen „***kontaktní osoby***“). Případnou změnu kontaktní osoby je smluvní strana povinna oznámit druhé smluvní straně do 5 pracovních dnů od provedení změny;
5. zajistit, aby kontaktní osoba dodavatele nejpozději do 30 dnů od nabytí účinnosti těchto Pravidel potvrdila písemně FN Brno k rukám „*kontaktní osoby FN Brno*, že všechny osoby podílející se na poskytování plnění této smlouvy za stranu dodavatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito Pravidly;
6. pokud při plnění předmětu smlouvy dodavatel zpracovává osobní údaje pro FN Brno, zavazuje se dodavatel uzavřít s FN Brno smlouvu o zpracování osobních údajů v souladu s Nařízením evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, nebo také „***GDPR***“) a zákonem č.110/2019 Sb., o zpracování osobních údajů v aktuálním znění.
7. dodavatel není oprávněn užít informace ani data obsažená v Systému, nebo v jiných systémech, které jsou plněním této smlouvy dotčeny, k jiným účelům než ke splnění závazků z této smlouvy. Informace či data dle předchozí věty může dodavatel využít k jiným účelům než k plnění této smlouvy jen po předchozím souhlasu FN Brno a jen v rozsahu FN Brno předem odsouhlaseném. Bude-li na základě této smlouvy pořízena databáze, je pořizovatelem takové databáze vždy FN Brno. Dodavatel je povinen informace a data obsažená v Systému, nebo v jiných systémech, které jsou plněním této smlouvy dotčeny, chránit proti jejich neoprávněnému užití třetí osobou.
8. při plnění smlouvy nesmí být využívány technologie, postupy ani systémy 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 ZKB, a které dle analýzy rizik představují kritické riziko; případné změny plnění v souladu s předchozí větou budou provedeny dodavatelem na základě pokynu FN Brno a na náklady dodavatele.
9. zaznamenávat podstatné okolnosti související s poskytovaným předmětem plnění dle smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.) a informovat o nich FN Brno.
10. zavést na své straně opatření pro ochranu zálohy dat vztahujících se k plnění smlouvy a pravidelně testovat funkčnost těchto záloh. Tato povinnost se nevztahuje na aplikační data Systému, ledaže smlouva stanoví jinak.
11. realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu smlouvy.
12. veškeré informace vyžadující vyšší míru ochrany[[1]](#footnote-1) poskytnuté FN Brno při poskytování plnění budou chráněny proti neautorizovanému přístupu; certifikáty a přístupová hesla nebudou uchovávány v nešifrovaném tvaru, pokud nebude mezi smluvními stranami v konkrétním případě dohodnuto jinak.
13. bude instalovat nový SW nebo nové verze SW pouze na základě FN Brno předem schválených migračních postupů[[2]](#footnote-2).

###### PERSONÁLNÍ BEZPEČNOST

1. pokud dodavatel využívá při poskytování plnění FN Brno poddodavatele, zavazuje se zajistit dodržování veškerých bezpečnostních opatření stanovených FN Brno rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se dodavatel zavazuje doložit FN Brno na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem, případně předložením čestného prohlášení o řádném naplňování této povinnosti.
2. dodavatel je povinen ve svých interních procesech a ve vztahu k osobám na své straně realizovat tato opatření:
	1. má stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah:
	2. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
	3. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;
	4. má určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;
	5. v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
	6. pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti;
	7. v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
	8. zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
	9. v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťuje předání odpovědností;
	10. hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;
	11. určuje pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
	12. vede o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

###### FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ

1. dodavatel se zavazuje dodržovat provozní řády areálů a budov (režimová opatření) FN Brno a využívaných prostor, se kterými byl prokazatelně seznámen, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty Systému anebo datové nosiče (dále také jen „***pracoviště***“).
2. dodavatel se zavazuje, že na pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k Systému.

###### DODRŽOVÁNÍ BEZPEČNOSTNÍ POLITIKY

1. dodavatel je povinen při plnění smlouvy dodržovat bezpečnostní politiky FN Brno a to počínaje okamžikem, kdy s nimi byl seznámen, a pouze v rozsahu, ve kterém s nimi byl seznámen.

###### ŘÍZENÍ PŘÍSTUPU

1. dodavatel bere na vědomí, že přístup k Systému je možné povolit pouze po evidenci osoby zastupující dodavatele v registru identit FN Brno nebo obdobném systému FN Brno, a to na základě požadavku dodavatele na přístup.
2. dodavatel bere na vědomí, že jeho zaměstnanec musí poskytnout své osobní údaje FN Brno, a to v rozsahu nutném pro zřízení přístupu, v opačném případě FN Brno není povinen přístup k Systému zaměstnanci dodavatele povolit. Dodavatel za účelem zajištění zákonnosti zpracování osobních údajů jeho zaměstnanců s přiděleným přístupem (fyzickým, logickým) k Systému, které za účelem plnění smluvních vztahů s dodavatelem provádí FN Brno, zajistí splnění informačních povinností vyplývajících z tohoto zpracování.
3. dodavatel bere na vědomí, že přidělení oprávnění zaměstnancům dodavatele musí být řízeno principem nezbytného minima a není nárokové.
4. nestanoví-li smlouva jinak, zavazuje se dodavatel, že udělený přístup nesmí být sdílen více osobami na jeho straně.
5. dodavatel se zavazuje, že vzdálený přístup do Systému bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.
6. dodavatel se zavazuje, že před připojením koncového zařízení, mobilního koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně FN Brno.
7. dodavatel se zavazuje, že bez zbytečného odkladu deaktivuje všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pokud daná činnost bude při plnění předmětu smlouvy vyžadována.
8. nedohodnou-li se smluvní strany v konkrétním případě jinak, zavazuje se dodavatel, že nebude instalovat a používat zejména typy nástrojů keylogger, sniffer, analyzátor zranitelností a port scanner, backdoor, rootkit a trojský kůň nebo jinou podobu malware.
9. dodavatel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury FN Brno, jsou a budou chráněny proti malware.
10. dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části Systému programový kód, který má za cíl nelegální ovládnutí, narušení, diskreditaci Systému ani nelegální získání dat nebo informací.
11. dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění FN Brno v Systému:
	1. neukládaly, nesdílely, data ani informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno FN Brno.
	2. nestahovaly, nesdílely, neukládaly, nearchivovaly a/nebo neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem.
	3. nezasílaly řetězové e-maily.
12. nestanoví-li smlouva jinak, zavazuje se dodavatel zajistit, aby osoby podílející se na poskytování plnění FN Brno, které přistupují do interní sítě nebo k Systému, měly ve svých externích zařízeních (např. notebook) aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
13. dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění FN Brno, které přistupují do interní sítě a/nebo k Systému chránily poskytnuté autentizační prostředky a údaje k systémům FN Brno. Dodavatel 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). Dodavatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost dodavatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy dodavateli či jiné osobě ze strany FN Brno.

###### ŘÍZENÍ ZMĚN A KONTINUITA ČINNOSTÍ

1. FN Brno v rámci řízení změn Systému přezkoumává možné dopady změn a určuje významné změny dle VKB. Dodavatel je povinen spolupracovat s FN Brno na řízení změn.
2. FN Brno 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 a zajistí možnost navrácení do původního stavu.
3. FN Brno má povinnost informovat dodavatele o výsledcích řízení změn, které mají dopady na plnění předmětu smlouvy ze strany dodavatele.
4. dodavatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn.
5. dodavatel se zavazuje poskytnout FN Brno 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.
6. v případě realizace penetračního testování Systému nebo testování zranitelnosti Systému poskytne dodavatel FN Brno za podmínek smlouvy veškerou potřebnou součinnost.
7. FN Brno má oprávnění zapojit dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí dodavatele do plánu kontinuity činností, který souvisí se Systémem, a/nebo zahrnout dodavatele do havarijního plánu FN Brno.

###### MONITOROVÁNÍ ČINNOSTÍ

1. dodavatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v systémovém prostředí FN Brno budou FN Brno průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na oprávněné zájmy FN Brno, jakož i s ohledem na obsah smlouvy a interních dokumentů FN Brno, se kterými byl dodavatel seznámen.

###### VÝMĚNA INFORMACÍ

1. pokud je předmětem smlouvy výměna informací mezi FN Brno a dodavatelem, musí být mezi smluvními stranami uzavřena dohoda o ochraně předmětných informací, ledaže je taková dohoda již součástí smlouvy nebo Pravidel.

###### SPECIFIKACE PODMÍNEK PRO FORMÁT PŘEDÁNÍ DAT, PROVOZNÍCH ÚDAJŮ A INFORMACÍ PO VYŽÁDÁNÍ FN BRNO

1. veškerá uživatelská a/nebo provozní data Systému dostupná dodavateli je dodavatel povinen FN Brno předat bez zbytečného odkladu po doručení žádosti o jejich poskytnutí nebo export, a to v elektronické, strojově čitelné podobě, v otevřeném formátu, jehož využití není zatíženo právy třetích osob a FN Brno jej může užít bez jakéhokoliv omezení. Nedohodnou-li se smluvní strany jinak, musí být součástí předávaných dat úplný popis formátu včetně datových typů a vzájemných vazeb v českém jazyce, ledaže by se jednalo o otevřený, standardizovaný formát. Neurčí-li FN Brno jinak, je dodavatel povinen data poskytnout v kódování českého jazyka UTF‑8.

###### ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTŮ

1. dodavatel se zavazuje, že při poskytování plnění pro FN Brno 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 FN Brno.
2. dodavatel 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 VKB.
3. dodavatel má povinnost neprodleně informovat FN Brno o kybernetických bezpečnostních incidentech a událostech souvisejících s plněním předmětu smlouvy, pokud se o nich dozvěděl nebo měl dozvědět. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu nebo události.
4. dodavatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit, případně minimalizovat pravděpodobnost jeho opakování.

###### OCHRANA DŮVĚRNÝCH INFORMACÍ

1. strany se zavazují zachovat mlčenlivost o veškerých informacích, osobních údajích, datech či zprávách, o nichž se dozvěděly v souvislosti s přípravou či plněním této smlouvy (dále jen „***důvěrné informace***“), a to včetně předmětu smlouvy, vlastní spolupráce a vnitřních záležitostí stran.
2. důvěrné informace ve smyslu této 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.
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 po ukončení této smlouvy.

###### KONTROLA A AUDIT DODAVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)

1. dodavatel se zavazuje poskytnout FN Brno veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z této smlouvy, jakož i ze ZKB a VKB, a za tímto účelem se zavazuje umožnit FN Brno provedení kontrol, včetně auditů prováděných FN Brno či auditorem, kterého FN Brno k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.
2. dodavatel je povinen FN Brno zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet zavedených technických a organizačních opatření.
3. dodavatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.
4. kontrola nebo audit mohou být provedeny v prostorách dodavatele nebo jeho poddodavatele a dodavatel má povinnost tyto kontroly nebo audity FN Brno či FN Brno pověřené osobě umožnit, přispět k nim a poskytnout FN Brno či FN Brno pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po dodavateli rozumně požadovat. Řádný audit lze provést maximálně jednou (1) za dva (2) roky. Mimořádnou kontrolu nebo audit může provádět FN Brno na základě písemné objednávky.
5. FN Brno má povinnost písmeně oznámit dodavateli provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu. Součástí oznámení bude i seznam osob, které jsou pověřeny ze strany FN Brno k provedení kontroly či auditu.
6. výstupem z provedené kontroly či auditu může být kontrolní/auditní zpráva; s jejími výsledky bude dodavatel seznámen a může se k nim vyjádřit.
7. dodavatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů.
8. dodavatel je povinen pravidelně provádět také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených FN Brno, a to na základě objednávky FN Brno nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytovaného plnění nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá dodavatel FN Brno bez zbytečného odkladu písemnou kontrolní zprávu.

###### SOULAD SMLOUVY S OBECNĚ ZÁVAZNÝMI PRÁVNÍMI PŘEDPISY

1. smlouva je uzavřena, s výjimkou právních předpisů upravujících kybernetickou bezpečnost, také v souladu s obecně závaznými právními předpisy platnými a účinnými k okamžiku uzavření této smlouvy, a dopadajícími na poskytované plnění. Dodavatel je povinen v průběhu plnění této smlouvy monitorovat změny těchto právních předpisů a poskytovat plnění v souladu s aktuálním zněním těchto právních předpisů.

###### ODSTOUPENÍ OD SMLOUVY

1. vedle důvodů sjednaných ve smlouvě, je FN Brno oprávněna odstoupit od této smlouvy rovněž tehdy, pokud dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení, nebo dojde ke změně vlastnictví či oprávnění nakládat s aktivy využívanými dodavatelem k plnění této smlouvy a tato změna bude FN Brno vyhodnocena jako nepřijatelné bezpečnostní riziko ve smyslu ZKB a/nebo VKB.

###### POVINNOSTI PŘI UKONČENÍ SMLOUVY, EXIT PLÁN, MIGRACE DAT

1. dodavatel se zavazuje poskytnout FN Brno veškerou potřebnou součinnost, dokumentaci a informace, s výjimkou informací, které nejsou významné z hlediska kybernetické bezpečnosti FN Brno a jsou součástí obchodního tajemství dodavatele ve smyslu § 504 občanského zákoníku, a které nejsou nezbytné k plnění povinností vyplývajících ze ZKB nebo VKB, účastnit se jednání s FN Brno a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, servisem a rozvojem předmětu smlouvy na FN Brno a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti této smlouvy, a to vše dle pokynů FN Brno (dále jen „***ukončení smlouvy***“).
2. součinnost bude spočívat zejména ve zpracování návrhu plánu předání a dále v součinnosti dodavatele v souvislosti s poskytováním služeb novým dodavatelem. Smluvní strany se přitom zavazují postupovat podle následujících pravidel:
	1. předložit FN Brno přehled vzájemných pohledávek z plnění poskytnutého v souladu se smlouvou do čtyřiceti pěti (45) kalendářních dnů od ukončení účinnosti smlouvy;
	2. neprodleně uhradit všechny případné nedoplatky vůči FN Brno;
	3. protokolárně vymazat nebo jinak zlikvidovat veškeré dodavateli dostupné kopie dat či provozních údajů, které byly dodavateli zpřístupněny nebo dodavatelem (jeho poddodavateli) vytvořeny na základě smlouvy nebo v souvislosti s plněním smlouvy, a to dle pokynů a v termínech stanovených dodavatelem. Dodavatel je povinen před likvidací předat všechna taková data a provozní údaje FN Brno; dodavatel umožní FN Brno dohled nad průběhem likvidace kopií dat a provozních údajů;
	4. předat FN Brno za účelem provádění správy Systému vlastními silami FN Brno veškeré přístupové a jiné údaje k Systému a nezbytnou technickou dokumentaci nejpozději k datu ukončení smlouvy, a to tak, aby FN Brno mohla Systém plně spravovat a provozovat;
	5. předat FN Brno všechny konfigurační soubory potřebné pro provoz Systému nejpozději k datu ukončení smlouvy;
	6. pokud bylo ukončeno veškeré poskytované plnění, na výzvu FN Brno zajistit odvoz všech technických prostředků ve vlastnictví dodavatele, které dodavatel užíval k poskytování plnění a které se nacházejí v prostorách FN Brno.

###### PRAVIDLA PRO LIKVIDACI DAT

1. dodavatel se zavazuje poskytnout FN Brno veškerou potřebnou součinnost pro likvidaci nepotřebných dat, za tím účelem smluvní strany dohodnou lhůty pro provádění likvidace dat, kde určí konkrétní rozsah a časové intervaly pro likvidaci dat. Smluvní strany sjednávají, že k likvidaci dat přistoupí po vzájemném odsouhlasení likvidace, podmínky likvidace musí být v souladu přílohou č. 4 VKB.

###### DŮSLEDKY PORUŠENÍ POVINNOSTI SMLUVNÍCH STRAN

1. Pro případ, že:
	1. dodavatel nesplní informační povinnost stanovenou mu tímto dodatkem, nebo
	2. dojde u dodavatele k významné změně kontroly nad osobou dodavatele, nebo
	3. dojde u dodavatele ke změně kontroly nad zásadními aktivy dodavatele využívanými k plnění smlouvy, nebo
	4. dodavatel zapojí do plnění smlouvy poddodavatele bez písemného povolení FN Brno

je FN Brno oprávněna odstoupit od smlouvy. Účinky odstoupení nastávají dnem doručení odstoupení od smlouvy dodavateli. Odstoupení nezbavuje dodavatele povinnosti poskytnout součinnost dle ustanovení těchto Pravidel při ukončení smlouvy.

1. pro případ porušení povinností dodavatele dle těchto Pravidel se sjednávají následující smluvní pokuty a sankce:
	1. pro případ porušení informační povinnosti stanovené těmito Pravidly je dodavatel povinen zaplatit FN Brno smluvní pokutu ve výši 50 000,- Kč za každé takové porušení,
	2. pro případ porušení některého z bezpečnostních opatření stanovených těmito Pravidly je dodavatel povinen zaplatit FN Brno smluvní pokutu ve výši 10 000,- Kč za každé takové porušení,
	3. pro případ porušení povinnosti dodavatele poskytnout součinnost stanovenou těmito Pravidly je dodavatel povinen zaplatit FN Brno smluvní pokutu ve výši 10 000,- Kč za každé takové porušení.

smluvní pokutou není dotčen nárok FN Brno na náhradu škody vzniklé v souvislosti s porušením smlouvy.

###### ÚPLATA ZA NĚKTERÁ PLNĚNÍ

1. povinnosti podle odst. 41 je dodavatel povinen plnit na základě výzvy FN Brno a pouze za úplatu, která se stanoví podle počtu člověkohodin potřebných na splnění povinnosti, přičemž na tomto počtu člověkohodin se smluvní strany dohodnou a sazba za člověkohodinu se určí podle smlouvy. Nelze-li sazbu za člověkohodinu určit podle smlouvy, nebo jestliže některá smluvní strana nesouhlasí se sazbou za člověkohodinu určenou podle smlouvy, určí se sazba za člověkohodinu dohodou smluvních stran. Nelze-li takové dohody dosáhnout, určí se sazba za člověkohodinu znaleckým posudkem zpracovaným osobou, na níž se smluvní strany dohodnou. Nedohodnou-li se smluvní strany na tom, kolik člověkohodin je potřebných na splnění povinnosti podle věty první, určí se tento počet člověkohodin znaleckým posudkem zpracovaným osobou, na níž se smluvní strany dohodnou. Náklady na zpracování znaleckých posudků podle tohoto odstavce se rozdělí mezi smluvní strany rovným dílem. Objednatelem těchto znaleckých posudků bude FN Brno, ledaže se smluvní strany dohodnou v konkrétním případě jinak. Splatnost faktur vystavených dodavatelem na základě tohoto odstavce je 60 dnů od vystavení. Dodavatel je povinen doručit fakturu FN Brno bez zbytečného odkladu po jejím vystavení.
1. Za informace vyžadující vyšší míru ochrany se ve smyslu této přílohy považují zejména identifikační údaje. [↑](#footnote-ref-1)
2. Migrační postup – soubor kroků definující převod dat mezi dvěma nebo více ISZS, nebo mezi dvěma nebo více verzemi téhož ISZS. [↑](#footnote-ref-2)