Příloha č. 7

Požadavky na dodavatele

Tento **Dokument** stanovuje v souladu s ustanovením § 4 odst. 4 zák. č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „**ZoKB**“) a § 8 odst. 1 písm. a) a f) ve spojení s přílohou č. 7 vyhl. č. 72/2018 Sb. (dále jen „**VoKB**“) závazná bezpečnostní opatření zohledňující požadavky systému řízení bezpečnosti informací, která se vztahují na dodavatele, kteří pro RBP, zdravotní pojišťovnu (dále jen „**RBP**“) výhradně či jako součást předmětu plnění dodávají, vyvíjí, implementují a/nebo provádějí servis software či hardware (dále také jen „**SW**“ či „**HW**“), a/nebo kteří v souvislosti s plněním pro **RBP** přistupují do informačního systému **RBP**, který byl určen významným informačním systémem (dále také„**VIS**“) v souladu se ZoKB a/nebo kteří v rámci poskytovaného plnění pro společnost **RBP** zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo uchovávají informace, data a/nebo provozní údaje **RBP**.

Účelem tohoto **Dokumentu** je dosažení společností **RBP** stanovené úrovně bezpečnosti informací v souladu s požadavky ZoKB, VoKB a dokumentace systému řízení bezpečnosti informací společnosti **RBP**.

**Dodavatelem** se pro účely tohoto **Dokumentu** rozumí každá osoba, jež poskytuje **RBP** jakékoliv plnění na základě Smlouvy. Dodavatelem se rozumí také provozovatel informačního nebo komunikačního systému a každý, kdo s **RBP** vstupuje do právního vztahu, nebo má s **RBP** uzavřenou smlouvu.

**Smlouvou** se pro účely tohoto **Dokumentu** rozumí smlouva uzavřená mezi **RBP** a dodavatelem.

**Aktivem** se pro účely tohoto **Dokumentu** rozumí primární aktivum, nebo podpůrné aktivum ve smyslu § 2 písm. f), nebo g) VoKB.

Není-li dále uvedeno jinak, rozumí se pojmy užívanými v tomto **Dokumentu** pojmy ve smyslu ZoKB, VoKB, nebo dokumentace systému řízení bezpečnosti informací ve společnosti **RBP**.

Pro účely tohoto **Dokumentu** se práva a povinnosti dodavatele stanovená tímto **Dokumentem** považují za bezpečnostní opatření.

Společnost **RBP** je správcem informačního systému základní služby ve smyslu ZoKB a VoKB. Dodavatel je povinen poskytovat plnění dle Smlouvy v souladu se všemi právními předpisy upravujícími kybernetickou bezpečnost ve společnosti **RBP** a v souladu se všemi vnitřními předpisy **RBP** upravujícími systém řízení bezpečnosti informací, resp. tak, aby se dodavatel vyvaroval jakékoliv činnosti, jež by mohla být označena za porušení uvedených právních předpisů a vnitřních předpisů **RBP**.

1. OBECNÉ POŽADAVKY BEZPEČNOSTI INFORMACÍ

Dodavatel je při poskytování plnění pro **RBP** povinen plnit následující povinnosti:

* 1. Postupovat v souladu s platnými právními předpisy.
	2. Dodavatel je povinen zachovat bezpečnost informací a dat obsažených v **VIS**, nebo v jiných informačních systémech, které jsou plněním Smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Dodavatel prohlašuje, že si je vědom všech povinností, které je povinen z hlediska zachování bezpečnosti informací v **RBP** dodržovat. Je-li nezbytné důvěrnost, dostupnost či integritu informací nebo dat omezit, ohrozit nebo přerušit, může tak dodavatel učinit pouze po předchozím souhlasu **RBP** a jen v rozsahu **RBP** předem odsouhlaseném.
	3. Dodavatel je povinen **RBP** písemně informovat o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy, a to do 15 pracovních dnů od nabytí účinnosti Smlouvy.
	4. Nestanoví-li dohoda stran jinak, dodavatel jmenuje nejpozději do 3 pracovních dnů po nabytí účinnosti Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních opatření a související komunikace mezi smluvními stranami.
	5. Zajistit, aby kontaktní osoba dodavatele nejpozději do 30 dnů od nabytí účinnosti Smlouvy potvrdila písemně **RBP**, že všechny osoby podílející se na poskytování plnění Smlouvy za stranu dodavatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s tímto **Dokumentem**.
	6. Zavést opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelně testovat funkčnost těchto záloh.
	7. V případě potřeby **RBP** musí dodavatel garantovat schopnost zrekonstruovat funkcionalitu aktiva do stavu požadovaného dle Smlouvy.
	8. Realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy.
	9. Průběžně detekovat technické zranitelnosti předmětu Smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat Objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Dodavatele. Nápravná opatření musí být schválena Objednatelem.
	10. Poskytovat **RBP** v termínech stanovených **RBP**, resp. bez zbytečného odkladu, požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje **SW** či po jeho předání.
	11. Dodat systémové a provozní bezpečnostní dokumentace**,** a to minimálně v následujícím rozsahu**:**
* provozní a bezpečnostní dokumentace,
* popis principů autentizace, autorizace a vytváření auditních stop,
* popis principů instalace a konfigurace,
* popis nezbytných bezpečnostních konfigurací,
* popis principů zálohování a archivace,
* plány kontinuity činností a havarijní plány.
	1. Veškeré informace vyžadující vyšší míru ochrany, zejména přístupová oprávnění, hesla, identifikační a jiné kritické údaje, poskytnuté **RBP** při poskytování plnění budou vhodným způsobem chráněny proti neautorizovanému přístupu; certifikáty a přístupová oprávnění nebudou uchovávány v nešifrovaném tvaru, pokud nebude mezi smluvními stranami pro konkrétní případ dohodnuto jinak.
	2. V produkčním prostředí systému **VIS** bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému **VIS**.
	3. Před spuštěním SW v produkčním prostředí daného **VIS** provede dodavatel kontrolu souladu daného **SW** s bezpečnostními opatřeními **RBP** a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného **SW** s bezpečnostními opatřeními, pokud byl s takovými opatřeními seznámen.
	4. Dodavatel odpovídá za to, že **SW** implementované do **VIS** budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace.
1. PERSONÁLNÍ BEZPEČNOST
	1. Pokud dodavatel využívá při poskytování plnění **RBP** poddodavatele, zavazuje se zajistit dodržování veškerých bezpečnostních opatření stanovených **RBP** ve smluvních vztazích se svými poddodavateli a tuto skutečnost doložit **RBP** na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem, případně předložením čestného prohlášení o řádném naplňování této povinnosti.
	2. Dodavatel a jeho případní poddodavatelé jsou povinni realizovat tato opatření:
* mít stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah;
* realizovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
* zajistit realizaci teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;
* v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
* v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pro osoby zastávající bezpečnostní role pravidelná odborná školení, zohledňující aktuální potřeby v oblasti kybernetické bezpečnosti;
* v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
* vést o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly;
* zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
* v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistit předání odpovědností;
* hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;
* určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
1. FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ
	1. Dodavatel se zavazuje, že na pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k **VIS**, který je předmětem plnění dle Smlouvy.
	2. Dodavatel se zavazuje dodržovat režimová opatření (provozní řády) budov a prostor zejména, kde jsou umístěna aktiva **VIS.**
2. OPRÁVNĚNÍ UŽÍVAT DATA a AUTORSTVÍ PROGRAMOVÉHO KÓDU
	1. Dodavatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Dodavateli Objednatelem za účelem plnění předmětu Smlouvy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy a zavazuje se nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a VoKB.
	2. Dodavatel se při poskytování plnění pro Objednatele zavazuje zajistit, aby při plnění Smlouvy dodržel podmínky stanovené zák. č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
3. KONTROLA A AUDIT DODAVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)
	1. Dodavatel se zavazuje poskytnout objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z tohoto **Dokumentu**, ze ZoKB a VoKB a umožnit objednateli provedení auditů prováděných objednatelem či pověřeným auditorem.
	2. Dodavatel je povinen Objednateli poskytnout nezbytnou součinnost a zpřístupnit veškerou potřebnou dokumentaci technických a organizačních opatření.
	3. Kontrola nebo audit mohou být provedeny u Dodavatele nebo jeho poddodavatele.
	4. Objednatel má povinnost písmeně oznámit Dodavateli provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu.
	5. Dodavatel je povinen pravidelně provádět kontrolu zavedených bezpečnostních opatření a hodnocení rizik.
	6. V případě neuspokojivých výsledků hodnocení dodavatele, nebo výsledků provedeného zákaznického auditu, musí dodavatel podniknout nezbytná opatření, která povedou k nápravě.
4. ŘETĚZENÍ DODAVATELŮ
	1. Dodavatel není oprávněn zapojit do plnění Smlouvy žádného dalšího poddodavatele bez předchozího povolení Objednatele.
	2. Dodavatel se zavazuje, že se bude řídit požadavky Objednatele na 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.
	3. Pokud Dodavatel využívá za účelem plnění předmětu Smlouvy poddodavatele, musí být tomuto poddodavateli uloženy na základě Smlouvy s Dodavatelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná tímto **Dokumentem** mezi Objednatelem a Dodavatelem.
	4. Dodavatel se zavazuje předložit Objednateli, na základě jeho písemného vyzvání, příslušnou smlouvu s poddodavatelem.
	5. Dodavatel má povinnost zajistit, že poddodavatel bude v souladu s požadavky, které Objednatel ukládá na základě tohoto **Dokumentu** Dodavateli.
5. ŘÍZENÍ PŘÍSTUPU
	1. Přístup k **VIS** je možné povolit pouze po evidenci osoby zastupující dodavatele v registru identit **RBP** nebo obdobném systému **RBP**, a to na základě požadavku dodavatele na přístup.
	2. Přidělení oprávnění zaměstnancům dodavatele musí být řízeno principem nezbytného minima a není nárokové.
	3. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci dodavatele ani poddodavatele.
	4. Nelze připojit koncové zařízení do sítě **RBP** bez předchozího schválení připojení určenou osobu na straně **RBP**.
	5. Dodavatel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury **RBP**, jsou a budou chráněny vhodným způsobem proti malware.
	6. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění **RBP**, které přistupují do interní sítě a/nebo **VIS** **RBP** chránily autentizační prostředky a údaje k **VIS** **RBP**. 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 **RBP**.
6. ŘÍZENÍ ZMĚN A KONTINUITA ČINNOSTÍ
	1. **RBP** 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 **VIS** a zajistí možnost navrácení do původního stavu.
	2. **RBP** má povinnost informovat dodavatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany dodavatele.
	3. Dodavatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn.
	4. Dodavatel se zavazuje poskytnout **RBP** 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.
	5. **RBP** má oprávnění zapojit dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí dodavatele do plánu kontinuity činností, který souvisí s **VIS** nebo s jeho **HW** komponentami a souvisejících služeb a/nebo zahrnutí dodavatele
	do havarijního plánu **RBP**.
7. MONITOROVÁNÍ ČINNOSTÍ
	1. Dodavatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v prostředí **RBP** budou průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na oprávněné zájmy **RBP**, jakož i s ohledem na obsah Smlouvy a interních dokumentů **RBP**, se kterými byl dodavatel seznámen.
8. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTŮ
	1. Dodavatel se zavazuje, že při poskytování plnění pro **RBP** 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 **RBP**.
	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 VoKB.
	3. Dodavatel má povinnost neprodleně informovat **RBP** o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.
	4. Dodavatel má povinnost provést analýzu příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
9. OCHRANA DŮVĚRNOSTI INFORMACÍ
	1. Smluvní strany se zavazují zachovat mlčenlivost o veškerých informacích a osobních údajích, o nichž se dozvěděly v souvislosti s plněním Smlouvy, a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí stran.
	2. Smluvní strany se zavazují, že zajistí, aby všechny osoby oprávněné zpracovávat informace a osobní údaje, o nichž se dozvěděly v souvislosti s plněním Smlouvy se zavázaly k mlčenlivosti. Závazek mlčenlivosti a ochrany důvěrnosti informací zůstává v platnosti i po ukončení Smlouvy.
10. INFORMAČNÍ POVINNOST DODAVATELE
	1. Dodavatel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy. Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.
	2. Dodavatel má povinnost informovat Objednatele o způsobu řízení rizik a o rizicích souvisejících s plněním předmětu Smlouvy, a to na základě písemné výzvy Objednatele.
	3. Dodavatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Dodavatele dle zák. č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv a změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy. V případě, že dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení, je **RBP** oprávněn odstoupit od Smlouvy.
11. POVINNOSTI PŘI UKONČENÍ SMLOUVY
	1. Dodavatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace při ukončení Smlouvy. Dodavatel se zavazuje, dle pokynů Objednatele, účastnit jednání s **RBP** a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, údržbou a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti Smlouvy.
12. SPECIFIKACE PODMÍNEK PRO FORMÁT PŘEDÁNÍ DAT, PROVOZNÍCH ÚDAJŮ A INFORMACÍ PO VYŽÁDÁNÍ RBP
	1. Veškerá uživatelská a/nebo provozní data **VIS** musí být **RBP** předána bez zbytečného odkladu po doručení žádosti o export, a to v elektronické, strojově čitelné podobě, v otevřeném formátu, jehož využití není zatíženo **RBP** právy třetích osob a **RBP** jej může užít bez jakéhokoliv omezení. Součástí předávaných exportovaných dat musí vždy být úplný popis formátu včetně datových typů a vzájemných vazeb v českém jazyce, ledaže by se jednalo o otevřený, standardizovaný formát. Pokud nestanoví **RBP** jinak, je dodavatel povinen data exportovat v kódování českého jazyka UTF-8. Soulad exportovaných dat s těmito požadavky a jejich úplnost, podléhá akceptaci **RBP**.
13. PRAVIDLA PRO LIKVIDACI DAT
	1. Dodavatel se zavazuje poskytnout **RBP** veškerou potřebnou součinnost pro likvidaci nepotřebných dat, za tím účelem smluvní strany dohodnou lhůty pro provádění likvidace dat, kde stanoví 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 VoKB.
14. SANKCE a DŮSLEDKY PORUŠENÍ POVINNOSTI SMLUVNÍCH STRAN
	1. Pro případ, že:
* dodavatel nesplní informační povinnost stanovenou mu tímto **Dokumentem**, nebo,
* dojde u dodavatele k významné změně kontroly nad osobou dodavatele, nebo,
* dojde u dodavatele ke změně kontroly nad zásadními aktivy dodavatele využívanými k plnění Smlouvy, nebo,
* dodavatel zapojí do plnění Smlouvy poddodavatele bez písemného povolení **RBP**,

je **RBP** oprávněna odstoupit od Smlouvy. Účinky odstoupení nastávají dnem doručení odstoupení od Smlouvy dodavateli. Odstoupení nezbavuje dodavatele povinnosti poskytnout součinnost dle ustanovení tohoto **Dokumentu** při ukončení Smlouvy.

* 1. Pro případ porušení povinností dodavatele dle tohoto **Dokumentu** se sankční ujednání řídí Smlouvou.