Příloha č. 3 Smlouvy o poskytnutí zabezpečeného úložiště s NIA autentizací – „Bezpečností opatření pro smluvní vztahy s významnými dodavateli“

1. Účel

1.1 Tato příloha stanoví způsoby a úrovně realizace bezpečnostních opatření pro zhotovitele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi objednatelem a zhotovitelem, a to v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**“), a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**vyhláška**“).

1.2 Další požadavky na objednatele a zhotovitele související s ochranou osobních údajů vyplývají z nařízení 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 (dále jen „**GDPR**“) a souvisejících právních předpisů (zákon č. 110/2019 Sb., o zpracování osobních údajů).

2. Bezpečnost informací

2.1 Smluvní strany jsou v souladu s čl. 6 smlouvy povinny zachovávat mlčenlivost o Chráněných informacích.

2.2 Zhotovitel je povinen provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti Systému a vést o něm bezpečnostní dokumentaci.

2.3 Zhotovitel se během poskytování plnění pro objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.

2.4 Povinnost mlčenlivosti se nevztahuje na informace:

a) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením smlouvy ze strany zhotovitele;

b) které jsou zhotoviteli známy a které měl zhotovitel prokazatelně volně k dispozici ještě před přijetím těchto informací od objednatele;

c) které budou následně zhotoviteli sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána;

d) jejich sdělení se vyžaduje ze zákona.

2.5 Zhotovitel se, nad rámec znění čl. 6 smlouvy, zavazuje plnit rovněž tyto povinnosti:

a) rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se podílejí na plnění smlouvy a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci a další osoby na straně zhotovitele podílející se na plnění

smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky objednatele, a to ještě před zahájením jakékoli činnosti;

b) přidělovat svým jednotlivým pracovníkům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (need-to-know principle), tedy dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele;

c) průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu u všech osob na straně zhotovitele, které přistupují k Systému;

d) průběžně detekovat bezpečnostní zranitelnosti a konfigurační nesoulady Systému a o zjištěných skutečnostech bez zbytečného odkladu informovat objednatele. Detekované bezpečnostní zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany zhotovitele. Nápravná opatření musí být schválena objednatelem.

3. Oprávnění užívat data, pravidla přístupu

3.1 Zhotovitel je při poskytování plnění oprávněn užívat data předaná objednatelem za účelem plnění předmětu smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu smlouvy.

3.2 Zhotovitel se při poskytování plnění pro objednatele zavazuje nakládat s daty (včetně osobních údajů) pouze v souladu se smlouvou, touto přílohou a příslušnými právními předpisy.

3.3 Zhotovitel odpovídá za aktuálnost seznamu pracovníků oprávněných přistupovat do objektů a Systému objednatele.

3.4 Zhotovitel bere na vědomí, že přidělení oprávnění zaměstnanci zhotovitele musí být řízeno principem nezbytného minima a není nárokové.

3.5 Zhotovitel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci zhotovitele nebo subdodavatele.

3.6 Zhotovitel se zavazuje, že vzdálený přístup do Systému bude vždy uskutečněn pouze prostřednictvím zabezpečeného VPN připojení.

3.7 Zhotovitel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části Systému programový kód, který má za cíl nelegální ovládnutí, narušení Systému nebo nelegální získání dat a informací.

3.8 Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, kteří přistupují do interní sítě objednatele, měli v externím zařízení (notebook/ počítač) aplikovány bezpečnostní záplaty a aktualizovanou antivirovou ochranu.

4. Autorství

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

5. Kontrola a audit

5.1 Zhotovitel se zavazuje poskytnout objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající ze smlouvy a této přílohy, jakož i ze ZKB a vyhlášky.

5.2 Zhotovitel se zavazuje umožnit objednateli provedení kontrol, včetně auditů v rozsahu minimálních požadavků podle ZKB a vyhlášky prováděných objednatelem či auditorem, kterého objednatel k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.

5.3 Kontrola nebo audit mohou být provedeny v prostorách zhotovitele nebo jeho subdodavatele a zhotovitel má povinnost tyto kontroly nebo audity objednateli či objednatelem pověřené osobě umožnit.

5.4 Objednatel má povinnost písemně oznámit zhotoviteli provedení kontroly nebo auditu, a to nejméně 14 dnů před provedením kontroly či auditu. Součástí oznámení bude i seznam osob, které jsou pověřeny ze strany objednatele k provedení kontroly nebo auditu.

5.5 Zhotovitel je srozuměn s pravidelným prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany objednatele.

6. Řetězení a řízení dodavatelů

6.1 V případě, že zhotovitel využívá při poskytování předmětu plnění subdodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající ze smlouvy a této přílohy.

6.2 Zhotovitel se zavazuje, že se bude řídit požadavky objednatele na řízení bezpečnosti informací a poskytne objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění subdodavatele, zajistí, že bude objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto subdodavatelů.

6.3 Zhotovitel odpovídá za to, že jeho subdodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími ze smlouvy a této přílohy; v případě, že dojde k nedodržení těchto požadavků ze strany subdodavatele zhotovitele, považuje se každé takové nedodržení požadavků za porušení povinnosti zhotovitele.

7. Dodržování bezpečnostní politiky Objednatele

7.1 Zhotovitel je povinen dodržovat bezpečnostní politiku objednatele, s jejímž obsahem byl seznámen.

7.2 Bezpečnostní politiky objednatele jsou měněny pouze v případě změn ZKB nebo vyhlášky.

8. Řízení změn

8.1 Zhotovitel se zavazuje poskytnout objednateli veškerou nezbytnou součinnost ke splnění povinností objednatele vyplývajících z ustanovení § 11 vyhlášky, zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testování a zajištění možnosti navrácení do původního stavu.

8.2 Objednatel u významných změn přezkoumává možné dopady změn, určuje významné změny podle vyhlášky, dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci.

8.3 Objednatel má povinnost informovat zhotovitele o výsledcích řízení změn, které mají dopady na plnění předmětu smlouvy ze strany zhotovitele.

9. Soulad s obecně závaznými právními předpisy

9.1 Zhotovitel se zavazuje poskytovat plnění předmětu smlouvy řádným způsobem a v souladu s platnými a obecně závaznými právními předpisy.

9.2 Způsob změny smlouvy v případě legislativních změn upravuje čl. 11 smlouvy.

10. Informační povinnost

10.1 Zhotovitel se zavazuje informovat objednatele o tom, jakým způsobem řídí bezpečnostní rizika spojená s plněním předmětu smlouvy a dále jaká jsou zbytková rizika s tím související.

10.2 Zhotovitel se při poskytování plnění pro objednatele zavazuje, že bude objednatele neprodleně, nejpozději do 2 kalendářních dnů, informovat o všech nově zjištěných kybernetických bezpečnostních incidentech souvisejících s předmětem plnění smlouvy, a to prostřednictvím kontaktních osob (čl. 9. odst. 9.7 smlouvy). Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

10.3 Zhotovitel se zavazuje, že při poskytování plnění pro objednatele stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat a bude hlásit všechny kybernetické bezpečnostní události a incidenty, včetně případů porušení zabezpečení osobních údajů, neprodleně po jejich detekci objednateli.

10.4 Zhotovitel je povinen realizovat opatření pro zvýšení odolnosti Systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom zejména z požadavků stanovených vyhláškou.

10.5 Zhotovitel se se během poskytování plnění pro objednatele zavazuje objednatele informovat o:

a) významné změně ovládání zhotovitele nebo jeho subdodavatele podle zákona č. 90 /2012 Sb., o obchodních korporacích, a to nejpozději do 3 pracovních dnů od uskutečnění této změny;
b) změně vlastnictví zásadních aktiv využívaných zhotovitelem k plnění smlouvy a změně oprávnění nakládat s těmito aktivy, a to nejpozději do 3 pracovních dnů od uskutečnění této změny.

11. Povinnosti při ukončení Smlouvy

11.1 V případě, že dojde k ukončení smluvního vztahu mezi smluvními stranami, zavazuje se zhotovitel, že i nadále bude dodržovat veškeré bezpečnostní požadavky stanovené právními předpisy, smlouvou a touto přílohou.

11.2 Zhotovitel se dále zavazuje, že vrátí objednateli veškerou důvěrnou dokumentaci, pokud mu byla předána a provede likvidaci a smazání dat, které vlastní zhotovitel z důvodu plnění smluvních závazků, vč. předání prohlášení o smazání objednateli.

11.3 Zhotovitel je povinen předat objednateli informace, které umožní provedení migrace dat zpracovávaných na prostředcích dodaných či zajišťovaných podle smlouvy na jiné systémy a současně zhotovitel poskytne objednateli informace, které jsou nezbytné k zajištění kontinuity služeb zajišťovaných prostředky, které byly předmětem smlouvy.

11.4 Zhotovitel se zavazuje poskytnout objednateli veškerou potřebnou součinnost při předání podle předchozího odstavce a současně se zavazuje účastnit se jednání s objednatelem a popř. třetími osobami za účelem plynulého a řádného převedení všech činností souvisejících s provozem, údržbou a rozvojem předmětu smlouvy na objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti smlouvy, a to vše podle pokynů objednatele.

12. Řízení kontinuity

12.1 Objednatel je oprávněn zapojit zhotovitele do řízení kontinuity činností, zejména je oprávněn k zahrnutí zhotovitele do plánu kontinuity činností, který souvisí se Systémem a souvisejících služeb a/nebo zahrnutí zhotovitele do havarijního plánu objednatele.

12.2 Objednatel má povinnost informovat zhotovitele o zapojení podle odst. 12.1 této přílohy.

13. Podmínky předávání dat

13.1 Veškeré provozní údaje, soubory, obsah logů, ostatní data a informace poskytnuté a zpracovávané v souvislosti s předmětem plnění smlouvy jsou ve výhradním vlastnictví objednatele.

13.2 Předávání dat musí probíhat tak, aby nemohly neoprávněné osoby údaje číst, kopírovat, měnit ani mazat. Běžné informace, klasifikované jako veřejné nebo interní, budou předávány prostřednictvím emailové komunikace, informace klasifikované jako citlivé pak prostřednictvím zabezpečeného cloudového úložiště objednatele.

13.3 Uchovávání předávaných dat na datových nosičích musí být zabezpečené proti přístupu neoprávněných osob.

14. Pravidla pro likvidaci dat

14.1 Objednatel se zavazuje stanovit pravidla pro mazání dat a likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií přiměřeně hodnotě a důležitosti aktiv.

14.2 Zhotovitel se zavazuje plnit požadavky objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů dat), která jsou v jeho sféře vlivu.

15. Sankce za porušení povinností

15.1 Sankce za porušení povinnosti mlčenlivosti ze strany zhotovitele je upravena v čl. 7 odst. 7.4 smlouvy.

15.2 Zhotovitel je povinen zaplatit objednateli smluvní pokutu ve výši 10.000,- Kč (slovy: „deset tisíc korun českých“) za každý jednotlivý případ porušení povinnosti v oblasti kybernetické bezpečnosti vymezený v této příloze.