

Příloha č. 2 Smlouvy – „Bezpečnostní opatření pro smluvní vztahy“

1. Účel

- 1.1 Tato příloha stanoví způsoby a úroveň realizace bezpečnostních opatření pro zhotovitele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi objednatelem a zhotovitelem, a to v souladu **ZKB**, a vyhláškou o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „**VoBO**“).
- 1.2 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, ve znění pozdějších předpisů).
- 1.3 Zhotovitel bere na vědomí, že součástí podmínek pro získání přístupu ke zdrojům objednatele je na straně objednatele zpracování osobních údajů zaměstnanců zhotovitele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude objednateli umožněno zpracovat osobní údaje dotčených zaměstnanců zhotovitele, nebude těmto zaměstnancům umožněn žádný přístup ke zdrojům objednatele.

2. Bezpečnost informací

- 2.1 Zhotovitel bere na vědomí, že objednatel má zaveden systém řízení bezpečnosti informací dle ZKB a ISO/IEC27001.
- 2.2 Zhotovitel je dále povinen provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti IS ÚOHS a vést o nich 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. V případě, že zhotovitel využívá při plnění smlouvy poddodavatele, zavazuje se zajistit adekvátní dodržování těchto bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli.
- 2.4 Smluvní strany jsou v souladu s čl. 6 smlouvy povinny zachovávat mlčenlivost o chráněných informacích.
- 2.5 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.

2.6 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 (poddodavatelé), zajištěním odpovídajícího vzdělávání prostřednictvím pravidelných školení a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci zhotovitele a poddodavatelé podílející se na plnění smlouvy musí být prokazatelně seznámeni s platnými interními předpisy a bezpečnostními požadavky objednatele, a to ještě před zahájením jakékoli činnosti podle smlouvy;
- b) přidělovat svým jednotlivým zaměstnancům 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 IS ÚOHS;
- d) průběžně detekovat bezpečnostní zranitelnosti a konfigurační nesoulady IS ÚOHS a o zjištěných skutečnostech bez zbytečného odkladu informovat objednatele. Detekované bezpečnostní zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy 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 svých zaměstnanců oprávněných přistupovat do objektů a IS ÚOHS objednatele za účelem plnění smlouvy.
- 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 poddodavatele.
- 3.6 Zhotovitel se zavazuje, že vzdálený přístup do IS ÚOHS bude vždy uskutečněn pouze prostřednictvím zabezpečeného VPN připojení.
- 3.7 Zhotovitel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části IS ÚOHS programový kód, který má za cíl nelegální ovládnutí, narušení IS ÚOHS nebo nelegální získání dat a informací.
- 3.8 Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, které přistupují do interní sítě objednatele, měly v externím zařízení (notebook/ počítač) aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu, dále nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové

a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem, nerealizovaly pokusy o neautorizovaný přístup ke zdrojům objednatele ani neoprávněnou modifikaci či jiné neoprávněné zásady do prostředků objednatele.

4. Kontrola a audit

- 4.1 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 VoBO.
- 4.2 Zhotovitel se zavazuje umožnit objednateli provedení kontrol, včetně auditů v rozsahu minimálních požadavků podle ZKB a VoBO 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.
- 4.3 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.
- 4.4 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.
- 4.5 Zhotovitel je srozuměn s pravidelným prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany objednatele.

5. Řetězení a řízení dodavatelů

- 5.1 V případě, že zhotovitel využívá při poskytování plnění subdodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající ze Smlouvy a této přílohy.
- 5.2 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 poddodavatele, zajistí, že bude objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů.
- 5.3 Zhotovitel odpovídá za to, že jeho poddodavatelé 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 a objednatel bude oprávněn požadovat smluvní pokutu dle článku 7 smlouvy.

6. Dodržování bezpečnostní politiky Objednatele

- 6.1 Zhotovitel je povinen dodržovat bezpečnostní politiky objednatele, s jejichž obsahem byl seznámen.
- 6.2 Bezpečnostní politiky objednatele jsou měněny pouze v případě změn ZKB nebo VoBO.

7. Řízení změn

- 7.1 Zhotovitel se zavazuje poskytnout objednateli veškerou nezbytnou součinnost ke splnění povinností objednatele vyplývajících z § 11 VoBO, 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.
- 7.2 Objednatel u významných změn přezkoumává možné dopady změn, určuje významné změny podle VoBO, dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci.
- 7.3 Objednatel má povinnost informovat zhotovitele o výsledcích řízení změn, které mají dopady na plnění smlouvy ze strany zhotovitele.

8. Informační povinnost

- 8.1 Zhotovitel se zavazuje informovat objednatele o tom, jakým způsobem řídí bezpečnostní rizika spojená s plněním smlouvy a dále jaká jsou zbytková rizika s tím související.
- 8.2 Zhotovitel se při poskytování plnění pro objednatele zavazuje, že bude objednatel neprodleně, nejpozději do 2 kalendářních dnů, informovat o všech nově zjištěných kybernetických bezpečnostních incidentech souvisejících s předmětem smlouvy, a to prostřednictvím kontaktních osob (čl. 9. odst. 9.3 Smlouvy). Součástí oznámení musí být datum a čas zjištění a popis povahy kybernetického bezpečnostního incidentu. Zhotovitel se dále zavazuje bez zbytečného odkladu a po dohodě s objednatelem a v dohodnutých termínech realizovat opatření požadovaná objednatelem ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu, který může mít dopad na objednatele.
- 8.3 Zhotovitel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků, jehož příčina je na straně zhotovitele, nebude posuzován jako okolnost vylučující odpovědnost zhotovitele za prodlení s řádným a včasným plněním této smlouvy a nebude důvodem k jakékoli náhradě případné újmy zhotovitele či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti zhotovitele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.
- 8.4 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 popsanych pravidel bude postupovat a bude hlásit všechny kybernetické bezpečnostní události a incidenty, včetně případů porušení zabezpečení osobních údajů, neprodleně po jejich detekci objednateli.
- 8.5 Zhotovitel je povinen realizovat opatření pro zvýšení odolnosti IS ÚOHS vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom zejména z požadavků stanovených VoBO.
- 8.6 Zhotovitel se během poskytování plnění pro objednatele zavazuje objednatel informovat o:
 - a) významné změně ovládání zhotovitele nebo jeho poddodavatele podle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, 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;
- c) žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána;
- d) fyzických osobách přicházejících do kontaktu s chráněnými informacemi objednatele (např. o osobách zastávající bezpečnostní role, penetrační testery a administrátory).

9. Dodržení pravidel bezpečného vývoje

- 9.1 Zhotovitel je ve fázi vývoje či údržby aktiv povinen zajistit řízení rizik dle VoBO a řídit významné změny v souladu s čl. 7 této přílohy, s důrazem na důkladné testování a dokumentaci změn.
- 9.2 Zhotovitel je povinen zajistit zejména oddělení provozního, vývojového a testovacího rozhraní.

10. Povinnosti při ukončení smlouvy

- 10.1 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.
- 10.2 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, a to nejpozději ke dni ukončení smlouvy.
- 10.3 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.
- 10.4 Zhotovitel se zavazuje poskytnout objednateli veškerou potřebnou součinnost při předání dat a informací 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 ukončení smlouvy, a to vše podle pokynů objednatele.

11. Řízení kontinuity

- 11.1 Objednatel je oprávněn zapojit zhotovitele do řízení kontinuity činností, zejména je oprávněn k zahrnutí zhotovitele do plánu kontinuity činností, který souvisí s IS ÚOHS a souvisejících služeb a/nebo zahrnutí zhotovitele do havarijního plánu objednatele. Zhotovitel se bude v rozsahu předmětu smlouvy aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření objednatele a za tímto účelem se zavazuje zajistit adekvátní

kontinuitu svých aktiv, která je potřebná k poskytování předmětu smlouvy, a pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

11.2 Objednatel má povinnost informovat zhotovitele o zapojení podle odst. 11.1 této přílohy.

12. Podmínky předávání dat

12.1 Veškeré provozní údaje, soubory, obsah logů, ostatní data a informace poskytnuté a zpracováváné v souvislosti s plněním smlouvy jsou ve výhradním vlastnictví objednatele.

12.2 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.

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

12.4 V případě, že bude zhotovitel požádán cizozemským orgánem o zpřístupnění nebo předání dat podle odst. 8.6 písm. c) této přílohy, zavazuje se zhotovitel jakékoliv zpřístupnění nebo předání dat provést až po přezkoumání zákonnosti žádosti a až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána, a to vše pouze v nezbytném rozsahu.

13. Pravidla pro likvidaci dat

13.1 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.

13.2 Zhotovitel se zavazuje plnit požadavky objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracováváných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů dat), která jsou v jeho sféře vlivu. Zhotovitel se zavazuje zajistit likvidaci dat ihned po pominutí účelu jejich zpracování nebo uložení. Po likvidaci dat uložených na datových nosičích nesmí být možné tyto data obnovit. O provedení likvidace musí zhotovitel vést protokol.