čj. SOAP/01-1622/2024-2

DODATEK Č. 1 KE SMLOUVĚ O POSKYTOVÁNÍ SLUŽEB
Č. SOAP/002-0468/2012
NA SERVIS VÝPOČETNÍ TECHNIKY A POČÍTAČOVÝCH SÍTÍ

podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

I.
Smluvní strany

Radomír Křen

Sídlo: Západní 422, 341 61 Kladruby
Zastoupená: Radomírem Křenem
IČ: 67894062
DIČ: [redacted]
Bankovní spojení:
Telefon:
Kontaktní osoby:
Kontaktní e-mail:
Zapsaná v živnostenském rejstříku magistrátu města Plzně.
(dále jen poskytovatel)

a

Česká republika – Státní oblastní archiv v Plzni

Sídlo: Sedláčkova 44, 306 12 Plzeň
Zastoupená: PhDr. Karlem Řeháčkem, Ph.D., ředitelem
IČ: 70979090
DIČ: CZ70979090, není plátcem DPH
Bankovní spojení: [redacted]
Telefon:
Kontaktní osoby: [redacted] informatici
Kontaktní e-mail:
(dále jen objednatel)

II.
Doplnění smlouvy

1. Předmětem tohoto dodatku smlouvy je doplnění přílohy č. 2 – Bezpečnostní opatření, která se nabytím účinnosti tohoto dodatku stává nedílnou částí smlouvy.
2. Tento dodatek smlouvy je vyhotoven ve dvou stejnopisech s vlastnoručními podpisy, z nichž jeden obdrží poskytovatel a jeden objednatel.
3. Obě smluvní strany prohlašují, že tento dodatek smlouvy uzavřely svobodně a vážně, jeho obsah považují za určitý a srozumitelný, jsou jim známy veškeré skutečnosti, jež jsou pro uzavření tohoto dodatku smlouvy rozhodující, na jeho ustanoveních dohodly jasně a určitě tak, aby kvůli nim nedošlo ke sporům, a že nebyl uzavřen v tísni, ani za jednostranně nevýhodných podmínek, na důkaz čehož připojují smluvní strany k tomuto dodatku smlouvy své podpisy.

V Plzni dne 23. 5. 2024
za poskytovatele:
[redacted]
Radomír Křen

V Plzni dne 23. 5. 2024
za objednatele:
[redacted]
PhDr. Karel Řeháček, Ph.D.
ředitel Státního oblastního archivu v Plzni

Příloha č. 2 – Bezpečnostní opatření

1. Úvod

Tato příloha smlouvy stanovuje bezpečnostní opatření zejména pro naplnění požadavků vyplývající se zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB"), 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 „VyKB") pro významné informační systémy resortu Ministerstva vnitra České republiky (dále jen „MV").

2. Bezpečnostní požadavky

2.1. Účel

1. Tato příloha smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro poskytovatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi objednatelem a poskytovatelem. Požadavky na poskytovatele jsou definovány dle platné právní úpravy, především pak dle ZoKB a VyKB.
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZoKB, VyKB, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek smlouvy zohledňující takové požadavky.

2.2. Obecné bezpečnostně provozní požadavky

Poskytovatel se při poskytování plnění pro objednatele zavazuje plnit následující povinnosti:

1. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro poskytovatele, jakožto významného dodavatele významného informačního systému, ze ZoKB a VyKB a reflektovat případné novely dotčených právních předpisů či novou právní úpravu, a bezpečnostními politikami stanovenými systémem řízení bezpečnosti informací (ISMS) objednatele dle specifikace předmětu veřejné zakázky;
2. kontaktní osoba poskytovatele uvedená ve smlouvě je zodpovědnou kontaktní osobou pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze smlouvy a této přílohy a související komunikace mezi smluvními stranami (dále také jen „kontaktní osoba pro bezpečnost na straně poskytovatele");
3. prokazatelně seznámit všechny osoby podílející se na poskytování plnění této smlouvy za stranu poskytovatele a/nebo jeho poddodavatelů s těmito bezpečnostními požadavky;
4. minimálně 1x ročně poskytnout součinnost objednateli při identifikaci a hodnocení aktiv a rizik významných informačních systémů souvisejících s předmětem plnění a na základě výsledků navrhnout a předložit objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik s přihlédnutím k výsledkům posuzování rizik i z hlediska dopadu na práva a svobody subjektů údajů;
5. dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných poskytovateli objednatelem, k jejímuž dodržování se poskytovatel zavázal, pokud byl poskytovatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob,

jakým byl s takovou dokumentací objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace poskytovateli, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu poskytovateli na sdílené úložiště aj.);

6. 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 poskytovatele podílející se na plnění smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky objednatele, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro objednatele v souvislosti s plněním této smlouvy;
7. zaznamenávat a na vyžádání objednateli poskytnout veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.);
8. přidělovat svým jednotlivým pracovníkům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět" (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele;
9. garantovat dostupnost, důvěrnost plnění a integritu předávaných dat s tím, že dodávané služby musí být v souladu s uzavřeným smluvním vztahem provozně monitorovány a vyhodnocovány;
10. průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně poskytovatele, které přistupují k předmětu plnění dle této smlouvy;
11. zavést opatření pro ochranu zálohy dat vztahujících se k plnění smlouvy a pravidelně (alespoň 1x za čtvrtletí, vždy ale s minimálně dvouměsíčním odstupem) testovat funkčnost těchto záloh;
12. průběžně detekovat, minimálně však jednou za 3 měsíce, technické zranitelnosti a konfigurační nesoulady předmětu plnění 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 poskytovatele, nápravná opatření musí být schválena objednatelem;
13. v případě napojení objednatele na dohledová centra zajistit rozhraní pro napojení a součinnost při zvládání kybernetických bezpečnostních událostí a incidentů;
14. uchovávat data o provozu (provozní a lokalizační údaje) v souladu s požadavky účinné legislativy ČR a dodržovat požadavky VyKB na obsah provozních událostí.

2.3. Oprávnění užívat data

1. Poskytovatel je při poskytování plnění pro objednatele oprávněn nakládat s daty předanými poskytovateli objednatelem výhradně za účelem plnění předmětu smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu smlouvy.
2. Poskytovatel se při poskytování plnění pro objednatele zavazuje nakládat s daty pouze v souladu se smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.

2.4. Kontrola souladu s požadavky bezpečnosti

1. Poskytovatel je srozuměn s prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany objednatele v souvislosti s poskytovanou službou poskytovatelem.
2. Hodnocení, kontrola a audit probíhají v intervalech stanovených objednatelem nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. Kontrola nebo audit mohou být provedeny v prostorách poskytovatele nebo jeho poddodavatele a poskytovatel má povinnost tyto kontroly a audity objednateli či objednatelem pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout objednateli či objednatelem pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po poskytovateli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.
3. Poskytovatel je povinen po zavedení opatření provést také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených objednatelem, na žádost objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá poskytovatel objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

2.5. Řetězení a řízení dodavatelů

Poskytovatel se při poskytování plnění pro objednatele zavazuje plnit následující povinnosti:

1. Poskytovatel nezapojí do poskytování plnění dle této smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení objednatele.
2. Poskytovatel 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.
3. Poskytovatel je povinen předat objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
4. Pokud poskytovatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky včetně požadavků na ochranu osobních údajů vyplývající z této smlouvy. Poskytovatel se zavazuje bezodkladně doložit objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této smlouvy.
5. Poskytovatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této smlouvy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele poskytovatele, považuje se každé takové nedodržení požadavků za porušení povinnosti poskytovatele dle této smlouvy.

2.6. Povinnosti v řízení změn dle ZoKB a VyKB

1. Poskytovatel se zavazuje v rozsahu předmětu plnění aktivně podílet na splnění povinností v oblasti řízení změn dle ZoKB a VyKB, zejména 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.

2. Poskytovatel se minimálně zavazuje v rozsahu předmětu plnění na své straně přiměřeně reagovat na změny na a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

3. Poskytovatel se zavazuje aktivně spolupracovat při testování významné změny.

2.7. Zvládání bezpečnostních událostí a incidentů

Poskytovatel se při poskytování plnění pro objednatele zavazuje, že:

1. stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci objednateli prostřednictvím ohlašovacích kanálů objednatele, v případech, kdy situace nestrpí odklad telefonicky; dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých nápravných opatřeních nad všemi částmi řešení, které jsou ve správě poskytovatele, a rizicích souvisejících s ohrožením kontinuity činností vést záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky objednatele a legislativy České republiky; nastavená pravidla a postupy podléhají schválení objednatelem;

2. nastavená pravidla pro zvládání bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získaní musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;

3. navrhne řešení tak, aby byl systém detekce a zvládání bezpečnostních událostí a incidentů začleněn do procesů a systémů a realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti;

4. v případě napojení objednatele na dohledová centra pro zvládání kybernetických bezpečnostních událostí a incidentů zajistí rozhraní pro napojení, zajistí součinnost a bude se řídit jeho pokyny;

5. provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2.8. Informační povinnost a povinnosti při výměně informací

1. Poskytovatel se během poskytování plnění pro objednatele zavazuje objednatele informovat o:

   a) způsobu řízení rizik, zbytkových rizicích souvisejících s plněním smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;

   b) významné změně ovládání poskytovatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných poskytovatelem k plnění na základě smluvního vztahu s objednatelem.

2. Poskytovatel se během poskytování plnění pro objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost před hrozbami v kybernetické bezpečnosti v souladu se ZoKB a VyKB.

2.9. Specifikace podmínek pro řízení kontinuity činností a zálohování a obnovu dat z pohledu ZoKB a VyKB

1. Poskytovatel se zavazuje poskytnout součinnost při zpracování plánu řízení kybernetických bezpečnostních incidentů (KBI) a plánu kontinuity a obnovy činností informačních systémů objednatele, které souvisí s předmětem plnění, včetně všech jejich komponent na základě zhodnocení a výsledků analýzy dopadů (Business Impact Analysis) vypracované v součinnosti s objednatelem.
2. Poskytovatel se zavazuje dodržovat požadavky objednatele na řízení kontinuity činností v souladu se ZoKB, VyKB a ustanoveními bezpečnostní politik, metodik a postupů předaných poskytovateli objednatelem.
3. Poskytovatel vypracuje a předá objednateli metodiku zálohování a obnovy dat (ve smyslu primárních aktiv) i systémů (resp. technických aktiv) ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. V případě požadavku objednatele poskytovatel zajistí, že záloha jako taková bude šifrována. Poskytovatel poskytne objednateli součinnost při pořízení a nasazení odpovídajícího technologického řešení, na kterém bude záloha a obnova dat prováděna.

2.10. Bezpečnost lidských zdrojů

1. Poskytovatel připraví poučení a zajistí poučení všech stran podílejících se na poskytování předmětu plnění o bezpečnostních pravidlech, jež se musí v průběhu dodávky dodržovat a zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů.
2. Poskytovatel se zavazuje zajistit nebo včas poskytovat součinnost objednateli, aby objednatel mohl zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávek, zastupitelnosti pracovníků, zejména kontaktní osoby pro bezpečnost na straně poskytovatele).

2.11. Požadavky na systémovou a provozní bezpečnostní dokumentaci

1. Nedílnou součástí poskytovaného plnění je součinnost při zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace a zpracování provozní dokumentace v souladu se ZoKB a VyKB.
2. V rámci součinnosti se poskytovatel zavazuje objednateli předat potřebné informace včetně identifikovaných datových toků, protokolů, architektonického nákresu systémů a jejich spolupráce, diagramu logického a fyzického zapojení a další dokumentaci předmětu plnění dle požadavku objednatele.

2.12. Fyzická ochrana a bezpečnost prostředí

1. Poskytovatel se zavazuje v budovách objednatele dodržovat režim návštěv v neveřejných prostorách a bezpečnostní požadavky na řízený přístup do bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče.
2. Poskytovatel se zavazuje, že v budovách objednatele neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění této smlouvy.

2.13. Požadavky na řízení přístupu

1. Poskytovatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem smlouvy je možné povolit pouze konkrétním fyzickým osobám (poskytovateli nebo zaměstnancům poskytovatele) na základě požadavku poskytovatele.
2. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno zásadou tzv. „potřeba vědět" (need-to-know principle) a není nárokové.
3. Poskytovatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny objednatelem.
4. Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací.
5. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli chránily autentizační prostředky a údaje k systémům objednatele.
6. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnosti vzniklé v důsledku porušení bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany poskytovatele. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.

2.14. Monitorování činností

Poskytovatel bere na vědomí, že plnění realizovaná v rámci plnění předmětu smlouvy nebo s ním úzce související mohou být objednatelem monitorovány a vyhodnocovány s ohledem na obsah smlouvy a interních dokumentů objednatele.

2.15. Likvidace dat

Poskytovatel se zavazuje plnit požadavky objednatele v oblasti likvidace dat dle přílohy č. 4 VyKB.