Dodatek č. 1 k Rámcové smlouvě na podporu digitalizace Krajského úřadu Jihočeského kraje

uzavřené dne 10.12.2024, ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „občanský zákoník“), ID smlouvy v Registru smluv: 29355856

Smluvní strany:

Jihočeský kraj

se sídlem: U Zimního stadionu 1952/2, 370 76, České Budějovice

zastoupený: MUDr. Martinem Kubou, hejtmanem kraje

IČO: 70890650

DIČ: CZ70890650

bankovní spojení: [redacted]

(dále jen „Objednatel“)

a

INADVISORS, s.r.o.

sídlo: Haštalská 791/9, 110 00, Praha 1

IČO: 28886127

DIČ: CZ28886127

[redacted]

zastoupený: Danielem Kadlecem, jednatelem

ID datové schránky: 22qbxup

(dále jen „Poskytovatel“)

(Objednatel a Poskytovatel – dále také jako „smluvní strany“)

uzavírají níže uvedeného dne, měsíce a roku na základě vzájemné shody tento Dodatek č. 1 k Rámcové smlouvě na podporu digitalizace Krajského úřadu Jihočeského kraje uzavřené dne 10.12.2024, ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „občanský zákoník“), ID smlouvy v Registru smluv: 29355856 (dále jen „Dodatek č. 1“).

Článek I.
Předmět Dodatku č. 1

1. Objednatel a Poskytovatel uzavřeli dne 10. 12. 2024, na základě výsledku výběrového řízení k veřejné zakázce s názvem „*Podpora digitalizace úřadu – rámcová smlouva*“ (dále jen „VZ“), Rámcovou smlouvu na podporu digitalizace Krajského úřadu Jihočeského kraje, ID smlouvy v Registru smluv: 29355856 (dále jen „**Smlouva**“).

2. Smluvní strany konstatují, že změny sjednané tímto Dodatkem č. 1 jsou realizovány v souladu s § 222 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, nepředstavují podstatnou změnu závazku ze smlouvy a nemění celkovou povahu veřejné zakázky. Důvodem změny je potřeba rozšíření objemu již sjednaných služeb v důsledku okolností vzniklých v průběhu plnění, které zadavatel nemohl při vynaložení náležité péče předvídat; jedná se zejména o vyšší komplexitu a rozsah činností souvisejících s digitalizací procesů a metodickou podporou. Změna je omezena na nezbytný rozsah, zachovává jednotkové ceny a ekonomickou rovnováhu smlouvy a je nezbytná pro řádné naplnění účelu veřejné zakázky.
3. Na straně Objednatele a Poskytovatele došlo ke změně kontaktní osoby.
4. Poskytovatel se zavazuje respektovat Bezpečnostní pravidla, Pravidla pro ochranu osobních údajů a Pravidla ochrany důvěrných informací stanovená Objednatelem, tak jak jsou specifikována v přílohách č. 1–4 tohoto Dodatku č. 1.

Článek II.
Změny Smlouvy

1. Vzhledem ke skutečnostem specifikovaným v čl. I. tohoto Dodatku č. 1 a vzhledem k naplnění zákonných i smluvních předpokladů se smluvní strany v souladu s ustanovením čl. 13., odst. 13.1. Smlouvy dohodly na následujících změnách Smlouvy.

a) Původní znění čl. 1. odst. 1.4 Smlouvy se ruší a nově zní takto:

„1.4 Předpokládaný rozsah prací je 157 MD (mandays). Služby budou čerpány podle potřeby objednatele.“

b) Původní znění čl. 3. odst. 3.2 Smlouvy se ruší a nově zní takto:

„3.2 Cena byla stanovena na základě nabídky Poskytovatele za 1 MD (manday). MD (mandays) budou čerpány dle potřeb objednatele až do výše předpokládané hodnoty VZ (3 mil. Kč bez DPH). K ceně bude připočtena DPH v souladu s právními předpisy.“

c) Původní znění čl. 11. odst. 11.1 Smlouvy se ruší a nově zní takto:

„11.1 Strany se dohodly, že bude ustanovena kontaktní osoba ze strany Objednatele a kontaktní osoba ze strany Poskytovatele. Ve věcech odborných, technických a při převzetí předmětu Smlouvy jsou určeny následující kontaktní osoby:

Na straně Objednatele:

[redacted]

Na straně Poskytovatele:

[redacted]

d) Původní znění čl. 13. odst. 13.6 Smlouvy se ruší a nově zní takto:

„13.6 Součástí této smlouvy jsou následující přílohy:

- Příloha č. 1 – Specifikace předmětu plnění
- Příloha č. 2 – Ochrana osobních údajů
- Příloha č. 3 – Bezpečnostní pravidla pro dodavatele

- Příloha č. 4 - Pravidla ochrany důvěrných informací“

Článek III.
Závěrečná ustanovení

1. Ostatní ustanovení Smlouvy tímto Dodatkem č. 1 nedotčená zůstávají beze změny.
2. Tento Dodatek č. 1 nabývá platnosti dnem podpisu poslední smluvní stranou a účinnosti dnem jeho uveřejnění v registru smluv.
3. Tento Dodatek č. 1 je vyhotoven v elektronické podobě, přičemž obě smluvní strany obdrží jeho elektronický originál.
4. Smluvní strany po přečtení tohoto Dodatku č. 1 potvrzují, že jeho obsah a práva a povinnosti odpovídají jejich pravé, vážné a svobodné vůli, a že Dodatek č. 1 byl uzavřen po vzájemném projednání.

V Českých Budějovicích dle elektronického podpisu	V Praze dle elektronického podpisu
Objednatel	Poskytovatel
Jihočeský kraj	**INADVISORS, s.r.o.**
[redacted]	[redacted]
MUDr. Martin Kuba, hejtman kraje	Daniel Kadlec, jednatel

Příloha č. 1 – Specifikace předmětu plnění

Hlavním účelem veřejné zakázky je podpořit procesy digitalizace správy dokumentů a výkonu spisové služby v organizaci zadavatele prostřednictvím metodické podpory a konzultačních služeb ve všech oblastech klíčových pro výkon spisové služby a správy dokumentů.

Předmět plnění veřejné zakázky zahrnuje analytické, metodické a konzultační služby a oblasti spisové služby, správy dokumentů a digitalizace oběhu dokumentů zadavatele, směřující k zajištění metodické podpory správné praxe při výkonu spisové služby a správy dokumentů, zaměřená zejména na následující oblasti:

a) Reengineering procesů zpracování dokumentů pře jejich digitalizací a zaváděním podpory ze strany informačních systémů

b) Metodická, technická a projektová podpora výkonu spisové služby, rozvoje elektronického systému spisové služby (dále „eSSL“) a dalších informačních systémů spravujících dokumenty (dále „ISSD“) na úrovni formulace procesních potřeb, specifikace zadání pro dodavatele rozvoje eSSL, definice testovacích scénářů a klíčových výkonnostních ukazatelů, ověření dodávek a jejich nasazení do produktivního provozu.

c) Zajištění efektivní metodické podpory uživatelů včetně přepracování a rozšíření uživatelské dokumentace zahrnující on-line nápovědu, stručné návody pro hlavní životní situace, online tutoriály a video návody, e-learning a další formy podpory uživatelů.

d) Podpora a rozvoj znalostí a dovedností uživatelů při správě dokumentů.

e) Monitoring a hodnocení výkonu spisové služby.

Předmětem veřejné zakázky je uzavření rámcové smlouvy na poskytnutí konzultačních služeb v jednotlivých definovaných rolích:

Role	Popis
Metodik spisové služby	Zajištění shody s právními předpisy a metodickými standardy výkonu spisové služby, sledování legislativních změn a souvisejících potřeb rozvoje eSSL, procesního a metodického zázemí KÚ JčK
Specialista – procesy spisové služby	Optimalizace procesů správy dokumentů, příprava na digitalizaci procesů, formulace business zadání pro rozvoj KÚ JčK.
Specialista – systémy spisové služby	Příprava technických řešení digitalizace procesů, formulace technického zadání pro rozvoj eSSL a dalších ISSD, ověřování shody dodávek se specifikovanými požadavky.
Projektový manažer	Řízení dodávky, koordinace s projektovým řízením dodávek rozvoje a podpory eSSL
Specialista vzdělávání v oblasti spisové služby a správy dokumentů	Zpracování koncepce vzdělávání a metodické podpory uživatelů, příprava vzdělávacích a podpůrných materiálů, realizace školení a workshopů směřujících k rozvoji kompetencí pracovníků KÚ JčK

Příloha č. 2 - Ochrana osobních údajů

1. Smluvní strany se zavazují, v souvislosti s touto smlouvou, postupovat v souladu s platným Obecným nařízením Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016 (dále jen „Nařízení“).

2. Poskytovatel bere na vědomí, že se ve smyslu Nařízení považuje a bude považovat za zpracovatele osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi. Objednatel je a bude nadále považován za správce osobních údajů.

3. Ustanovení o vzájemných povinnostech správce a zpracovatele při zpracování osobních údajů zajišťuje, že nedojde k nezákonnému použití osobních údajů týkajících se subjektů údajů ani k jejich předání do rukou neoprávněné třetí strany. Smluvní strany se dohodly na podmínkách zajištění odpovídajících technických a organizačních opatření k zabezpečení ochrany osobních údajů a základních práv a svobod subjektů údajů při zpracování osobních údajů zpracovatelem, a to zejména s ohledem na povahu, rozsah a účel zpracování, jakož i na rizika pro práva a svobody fyzických osob.

4. Zpracovatel se zavazuje zpracovávat pouze a výlučně ty osobní údaje, které jsou nezbytné k výkonu jeho činnosti dle této smlouvy, zejména identifikační a kontaktní údaje subjektů údajů a případně další údaje nezbytné k plnění smlouvy. Subjekty údajů jsou zejména zaměstnanci správce a další osoby, jejichž údaje jsou nezbytné pro plnění této smlouvy a dále osoby, jejichž adresní a identifikační údaje jsou obsaženy v kartotéce eSSL. Osobní údaje subjektů budou zpracovávány zejména v následujícím rozsahu: jméno, příjmení, osobní číslo, adresa pracoviště, oddělení, IP adresa, firemní emailová adresa zaměstnance, jméno, příjmení, adresa, datum narození, identifikátor datové schránky, e-mail adresátů a odesílatelů.

5. Zpracovatel je oprávněn zpracovávat osobní údaje pouze po dobu účinnosti smlouvy a dále po dobu nezbytnou k vypořádání práv a povinností z ní vyplývajících, nejdéle však po dobu stanovenou právními předpisy nebo pokyny správce.

6. Zpracovatel je oprávněn zpracovávat osobní údaje pouze za účelem plnění této smlouvy, zejména za účelem poskytování sjednaných služeb, jejich administrace a komunikace se správcem a subjekty údajů. Povahou zpracování osobních údajů je zejména jejich shromažďování, předávání, ukládání, uchovávání, organizace, strukturování, nahlížení, používání, vyhledávání, případné zpřístupnění oprávněným osobám a výmaz nebo likvidace, a to jak manuálně, tak pomocí automatizovaných prostředků.

7. Zpracovatel je povinen se při zpracování osobních údajů řídit doloženými pokyny správce. Za písemnou formu se považuje i elektronická komunikace. Zpracovatel je povinen neprodleně správce informovat, pokud dle jeho názoru udělený pokyn porušuje Nařízení nebo jiné právní předpisy.

8. Zpracovatel je povinen zajistit, že osoby, jimiž bude provádět plnění dle této smlouvy, se zavážou k mlčenlivosti ve vztahu ke všem osobním údajům, ke kterým budou mít přístup nebo s nimi přijdou do kontaktu.

9. Zpracovatel je povinen přijmout vhodná technická a organizační opatření k zabezpečení osobních údajů, zejména řízení a evidenci přístupových oprávnění, zabezpečení systémů prostřednictvím autentizačních prvků, ochranu proti neoprávněnému přístupu, pravidelné zálohování dat, ochranu proti ztrátě, poškození nebo zneužití údajů, používání bezpečnostního software a přijetí a dodržování interních pravidel ochrany osobních údajů.

10. Zpracovatel je povinen neprodleně informovat správce o jakémkoliv porušení zabezpečení osobních údajů nebo podezření na něj.

11. Zpracovatel není oprávněn zapojit dalšího zpracovatele bez předchozího písemného souhlasu správce a je povinen zajistit, aby další zpracovatel byl vázán stejnými povinnostmi.
12. Zpracovatel je povinen poskytovat správci součinnost při plnění povinností podle Nařízení, zejména bezodkladně informovat správce o žádosti subjektu údajů, nejednat bez pokynu správce, poskytovat součinnost při vyřizování práv subjektů údajů a při zajištění souladu s články 32 až 36 Nařízení. Současně je povinen na vyžádání zpřístupnit správci informace o přijatých technických a organizačních opatřeních a umožnit kontrolu jejich dodržování.
13. Po skončení účinnosti smlouvy je zpracovatel povinen osobní údaje vymazat nebo je předat správci a vymazat jejich kopie, pokud právní předpis nestanoví jinak.

Příloha č. 3 - Bezpečnostní pravidla pro dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva Jihočeského kraje a Krajského úřadu Jihočeského kraje (dále jen „**Objednatel**“), ke kterým mají přístup Dodavatelé.

Základní odpovědnosti Dodavatele

Dodavatel řešení:

1. Je povinen postupovat v souladu s platnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro Objednatele, jakožto registrovaného poskytovatele regulované služby v odvětví veřejná správa ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „Zákon“) a vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „Vyhláška“) a reflektovat případné novely uvedených právních předpisů či novou právní úpravu.
2. Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost Objednatele, zabránilo bezpečnostním incidentům a krizovým situacím.
3. Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
4. Je povinen zajistit, aby předmět plnění nebyl 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 Zákonem, a které dle analýzy rizik představují vysoké riziko.
5. Je povinen provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu Smlouvy (dodávaného řešení) a na základě výsledků navrhovat a předkládat Objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik.
6. Je povinen zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro Objednatele.
7. Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s Objednatelem.

Ochrana Aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím Objednatele musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků Objednatele zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

Řízení přístupu k ICT/IS

1. Přihlášení Dodavatele do sítě Objednatele musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci.
2. Dodavatel se zavazuje, že před připojením koncového zařízení, mobilní 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 Objednatele.
3. Dodavatel se zavazuje, že vzdálený přístup do systému Objednatele bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

4. Dodavatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.
5. Dodavatel se zavazuje, že nebude instalovat a používat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.
6. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednatele, kteří přistupují do interní sítě nebo informačního systému Objednatele, měli v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
7. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo Poddodavatele.
8. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu.

Kontrola a Audit dodavatele

1. Dodavatel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z těchto pravidel, jakož i ze Zákona a Vyhlášky, a za tímto účelem se zavazuje umožnit Objednateli provedení kontrol, včetně auditů prováděných Objednatelem či auditorem, kterého Objednatel k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.
2. Dodavatel je povinen Objednateli zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet technických a organizačních opatření.
3. Dodavatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.
4. Dodavatel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů (např. Národnímu úřadu pro kybernetickou a informační bezpečnost).
5. Dodavatel se zavazuje umožnit Objednateli provést po vzájemné dohodě v rozsahu předmětu plnění testy dostupnosti, důvěrnosti a integrity dat, informací a jiných zdrojů Dodavatele, které jsou využívány k poskytování předmětu plnění, a poskytnout potřebnou součinnost.
6. Dodavatel se zavazuje zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu s těmito Bezpečnostními požadavky.

Ochrana před škodlivým softwarem

Dodavatel je povinen:

1. Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK. Standardy KÚ JK se řídí Zákonem a zejména Vyhláškou a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.
2. Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury dodavatele.
3. Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.
4. Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

Poddodavatelé

1. Dodavatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího Poddodavatele bez předchozího konkrétního nebo obecného povolení Objednatele.

2. Dodavatel je povinen předat Objednatele kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
3. Dodavatel má povinnost zajistit, že Poddodavatel bude v souladu s požadavky, které Objednatele ukládá na základě těchto Bezpečnostních pravidel Dodavateli.
4. Dodavatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z těchto Bezpečnostních pravidel; v případě, že dojde k nedodržení těchto požadavků ze strany Poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle Smlouvy.
5. Využití třetí osoby k plnění předmětu smlouvy nebo její části nezbavuje Dodavatele odpovědnosti za případnou škodu způsobenou Objednateli.

Řízení změn

1. Dodavatel se zavazuje určovat významné změny, za které se považují změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost a představují vysoké riziko. Dodavatel je povinen o těchto významných změnách předem informovat Objednatele.
2. U významných změn se Dodavatel zavazuje zejména:
    a. provádět analýzu rizik,
    b. přijímat opatření za účelem snížení negativních dopadů těchto změn, včetně případného penetračního testování a testování zranitelnosti,
    c. dokumentovat jejich řízení,
    d. aktualizovat specifickou bezpečnostní politiku pro danou v oblast,
    e. zajistit možnost navrácení do původního stavu.
3. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Dodavatel Objednateli veškerou potřebnou součinnost. Dodavatel je povinen přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

Řízení bezpečnostních rizik

1. Dodavatel je povinen alespoň 1x ročně provádět vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. O výsledku hodnocení rizik Dodavatel Objednateli předloží Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
    a. vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok, včetně vyhodnocení souladu s těmito Bezpečnostními požadavky,
    b. identifikaci a hodnocení rizik s vazbou na předmět plnění,
    c. realizovaná bezpečnostní opatření,
    d. nepokrytá bezpečnostní rizika a návrh opatření,
    e. vyhodnocení bezpečnostních událostí a incidentů.

Monitorování činností

1. Dodavatel bere na vědomí, že veškerá jeho aktivita realizovaná v informačních systémech, může být Objednatelem průběžně a pravidelně monitorována.
2. Předmět plnění musí poskytovat auditní záznamy (logy) o činnostech v něm provedených, v rozsahu stanoveném Vyhláškou, které umožní jednoznačně určit uživatele, čas a provedenou činnost.
3. Dodavatel se zavazuje, že umožní přístup k auditním údajům (systémové a aplikační logy) v takové podobě a formátu, který je možné dále zpracovávat v rámci systému nástrojů SIEM (Security Information Event Management) a tyto bude pravidelně předávat Objednateli.

Zvládání kybernetických bezpečnostních incidentů

1. Dodavatel se zavazuje, že bude hlásit všechny nestandardní situace, bezpečnostní slabiny, kybernetické bezpečnostní události (KBU) a kybernetické bezpečnostní incidenty (KBI) včetně

případů porušení zabezpečení osobních údajů bez zbytečného odkladu po jejich detekci Objednateli.

2. Hlášení KBU a KBI provádí Dodavatel telefonicky nebo e-mailem na kontakty uvedené ve smlouvě. Součástí oznámení musí být popis povahy konkrétního případu (KBU nebo KBI).
3. Pokud dojde ke KBU nebo ke KBI a následnému zvládání a vyhodnocování KBI s ohledem na bezpečnost na straně Objednatele, poskytne Dodavatel Objednateli požadovanou součinnost např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem).
4. Dodavatel má povinnost provést analýzu příčin KBU nebo KBI a navrhnout opatření s cílem zamezit jeho opakování v případě, že Dodavatel KBU nebo KBI zapříčinil nebo se na jeho vzniku podílel.
5. Dodavatel má povinnost uchovávat informace o KBU a KBI pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
6. Dodavatel se zavazuje stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání KBU a KBI.
7. Dodavatel se zavazuje v případě vzniku KBI a následného zvládání a vyhodnocování KBI a/nebo v případě podezření na KBI poskytnout Objednateli součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele.
8. Dodavatel bere na vědomí, že postup zvládání KBU nebo KBI či jiný důsledek porušení těchto Bezpečnostních pravidel, jehož příčina je na straně Dodavatele, nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Dodavatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.

Akvizice, vývoj a údržba

1. Dodavatel se zavazuje zejména:
    a. zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění smlouvy,
    b. předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
        i. dokumentace skutečného provedení,
        ii. dokumentace všech bezpečnostních nastavení, funkcí a mechanismů,
        iii. dokumentace obsahující popis autorizačního konceptu a oprávnění,
        iv. dokumentace obsahující zálohovací a archivační postupy,
        v. dokumentace obsahující instalační a konfigurační postupy,
        vi. dokumentaci pro zajištění kontinuity provozu a obnovy po havárii.

Informační povinnost dodavatele

1. Dodavatel má povinnost bez zbytečného odkladu informovat Objednatele o významné změně ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv, jakož i změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy.
2. Dodavatel má povinnost informovat Objednatele o způsobu řízení rizik, jakož i o zbytkových rizicích souvisejících s plněním předmětu Smlouvy.

Výměna informací

1. Dodavatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů.

2. Dodavatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

Řízení kontinuity činností

1. Dodavatel zavazuje zejména:
    a. určit minimální úroveň poskytovaných služeb přijatelnou z hlediska zajištění kontinutity poskytovaných činností,
    b. určit dobu obnovení chodu, během které bude po bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb dle písm. a),
    c. určit časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
    d. vypracovat, aktualizovat a pravidelně testovat plány kontinuity činnosti a havarijní plány související s poskytováním předmětu plnění,
    e. Objednatel má oprávnění zapojit Dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Dodavatele do plánu kontinuity činností včetně jeho testování, který souvisí s daným IS a včetně souvisejících služeb a/nebo zahrnutí Dodavatele do havarijního plánu Objednatele.
2. Dodavatel předloží Objednateli metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována.

Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti Objednatele, který má právo výjimku udělit.

Likvidace dat

Pokud v rámci plnění předmětu Smlouvy má Dodavatel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pravidly pro mazání dat a v souladu se způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií na základě tabulky č.1. Přičemž, pokud není určena klasifikace informace, bude použit způsob likvidace pro důležitost aktiva kritickou.

Povinnosti při ukončení smlouvy

1. Dodavatel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, podporou a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti této Smlouvy, a to vše dle pokynů Objednatele (dále jen „**Ukončení smlouvy**“).
2. Dodavatel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat Objednateli dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „**Plán**“). Dodavatel se zavazuje Plán po dobu trvání této Smlouvy průběžně aktualizovat a Objednatele vždy při změně jakékoliv skutečnosti uvedené v Plánu předat aktualizovanou verzi Plánu zohledňující tuto změnu.
3. Dodavatel se zavazuje min. 1 x ročně provést export dat v Objednatelem odsouhlasené struktuře, současně předá Objednateli popis struktury dat v podobě, která bude pro Objednatele čitelná a pochopitelná a umožní Objednateli import dat do jiného Objednatelem vybraného systému/řešení.
4. Dodavatel je povinen poskytnout plnění nezbytná k realizaci tohoto Plánu za přiměřeného použití vhodných ustanovení této Smlouvy. Závazek dle tohoto ustanovení platí i po ukončení této Smlouvy.

5. Strany se dohodly, že cena za vypracování Plánu a poskytnutí plnění nezbytného k realizaci Plánu je součástí ceny dle této Smlouvy.

Závěrečná ustanovení

Tato Bezpečnostní pravidla jsou v souladu s platnými právními předpisy České republiky. Pokud se jakékoli ustanovení těchto Bezpečnostních pravidel stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení těchto Bezpečnostních pravidel a rovněž Smlouvy. Strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a těchto Bezpečnostních pravidel jako celkem.

Informace o verzi

Schváleno: [redacted] 3. zástupce ředitele Krajského úřadu Jihočeského kraje, Manažer kybernetické bezpečnosti

Datum: 16.04.2025

Tabulka č. 1

	Přípustný způsob likvidace podle úrovně důležitosti aktiva			
Nosič informace	**1. Nízká**	**2. Střední**	**3. Vysoká**	**4. Kritická**
Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)	Odstranění: Vyhození do odpadu.	Přepsání: Začernění.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.	
		Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.		
Mobilní zařízení (mobilní telefony, tablety)	Odstranění: Vymazání informací, reset zařízení do továrního nastavení.	Přepsání: Pro zařízení s šifrovaným úložištěm – odstranění informací a reset do továrního nastavení.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.	
Síťová zařízení (router, switch, modem a podobně)	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).		
Kancelářské vybavení (scanery, tiskárny, fax)				
Magnetická média (magnetické	Odstranění: Smazání dat na úrovni	Přepsání: Přepsání dat. V případě		

<table>
<tr><td>pásky, disky, HDD [Hard Disk Drive])</td><td rowspan="3">souborového systému.</td><td rowspan="2">šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů</td><td colspan="2"></td></tr>
<tr><td>Optická média (CD, DVD, HD-DVD, BLU-RAY)</td><td colspan="2" rowspan="2">Fyzická likvidace: Zničení nosiče informací.</td></tr>
<tr><td>Elektronická média (flash paměti)</td><td>Fyzická likvidace.</td></tr>
<tr><td rowspan="3">Outsourcing a cloud</td><td colspan="4">Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.</td></tr>
<tr><td rowspan="2">Odstranění: Odstranění všech souborů včetně předchozích verzí.</td><td>Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.</td><td rowspan="2">Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.</td><td rowspan="2">Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií podle výše uvedených řádků pro úroveň kritická.</td></tr>
<tr><td>Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.</td></tr>
</table>

Příloha č. 4 - Pravidla ochrany důvěrných informací

Tento dokument upravuje pravidla pro nakládání s důvěrnými informacemi, které si smluvní strany vzájemně poskytují v souvislosti se spoluprací a vzájemnou komunikací.

1. Předmět úpravy

1.1. Tento dokument upravuje práva a povinnosti při ochraně důvěrných informací (jak jsou dále definovány v čl. 2.1), které jedna smluvní strana jako poskytovatel důvěrné informace poskytne druhé smluvní straně jako příjemci důvěrné informace, nebo které si smluvní strany vzájemně poskytnou v souvislosti se spoluprací podle „Dodatku č. 1 k Rámcové smlouvě na podporu digitalizace Krajského úřadu Jihočeského kraje“ ze dne 09.06.2026 (dále jen „spolupráce“).

2. Definice důvěrné informace

2.1. Důvěrnými informacemi se rozumí veškeré informace související s činností smluvních stran, bez ohledu na formu jejich poskytnutí nebo zachycení (včetně umožnění přístupu k takovým informacím v elektronické formě), které nejsou veřejně známé a o nichž se příjemce důvěrné informace dozví nebo dozvěděl, případně je obdrží nebo obdržel, a to v jakékoli formě, a to zejména:

2.1.1. skutečnosti tvořící obchodní tajemství ve smyslu § 504 zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“) a důvěrné údaje a sdělení ve smyslu § 1730 občanského zákoníku,

2.1.2. informace, jež nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle poskytovatele důvěrné informace utajeny a příjemce důvěrné informace odpovídajícím způsobem jejich utajení zajišťuje,

2.1.3. skutečnosti týkající se zákazníků, obchodních partnerů a zaměstnanců smluvních stran, jejich činnosti a vztahů k dalším subjektům,

2.1.4. a dále následující informace: obsah obchodních nebo marketingových nabídek nebo studií, obsah cenových nebo platebních podmínek, návrhy a znění smluv, podnikatelské záměry, hospodářská a finanční situace, analýzy vypracované nebo zadané k vypracování jednou ze smluvních stran, informace uložené v informačních systémech poskytovatele důvěrné informace, informace o veškeré ICT infrastruktuře poskytovatele důvěrné informace včetně informací spojených s jejím provozem, informace se zvláštním režimem utajení (utajované skutečnosti, bankovní tajemství, telekomunikační tajemství, osobní údaje fyzických osob).

2.2. Pro vyloučení pochybností se stanoví, že Důvěrné informace není nutné výslovně označovat. Za účelem vyloučení pochybností o jejich charakteru informací je však jejich označení vhodné, zejména v případech, kdy by příjemci důvěrné informace nemusel být charakter informací jednoznačně zřejmý.

2.3. Za Důvěrné informace se nepovažují informace, které jsou nebo se stanou veřejně dostupnými jinak než porušením povinností mlčenlivosti, nebo k jejichž sdělení poskytovatel důvěrné informace udělí předchozí písemný souhlas.

3. Práva a povinnosti

3.1. Příjemce důvěrné informace se zavazuje, že po dobu trvání spolupráce a dále po dobu pěti let od jejího ukončení, přímo ani nepřímo sám či prostřednictvím svých orgánů, zaměstnanců, spolupracovníků, zástupců, poradců ani jiných třetích osob bez předchozího písemného souhlasu poskytovatele důvěrné informace nezveřejní ani jinak nesdělí jakékoliv třetí osobě (s výjimkou osob, kterým mohou být informace zpřístupněny podle tohoto dokumentu) ani jí neumožní jakkoliv využít jakoukoliv Důvěrnou informaci a bude Důvěrné informace udržovat v tajnosti a nebude je zneužívat v neprospěch poskytovatele důvěrné informace či k jeho škodě ani je nebude využívat jinak než k účelu spolupráce uvedené v článku 1.1.

3.2. Povinnost podle předchozího odstavce se v rozsahu nezbytném pro plnění úkolů v rámci spolupráce nevztahuje na zaměstnance, spolupracovníky, auditory nebo poradce příjemce důvěrné informace, vždy však za podmínky, že tyto osoby budou vázány obdobnou povinností mlčenlivosti a příjemce důvěrné informace odpovídá za jejich jednání, jako by jednal sám.
3.3. Příjemce důvěrné informace se zavazuje používat přiměřenou míru péče, avšak v žádném případě ne v menší míře, než je míra péče, kterou využívá k ochraně svých Důvěrných informací a informací vlastnických, které jsou podobného významu, k ochraně neoprávněného užívání, poskytnutí, zveřejnění nebo šíření Důvěrné informace.
3.4. Příjemce důvěrné informace může poskytnout nebo zpřístupnit Důvěrnou informaci bez předchozího souhlasu poskytovatele důvěrné informace pouze v případě, že mu takovou povinnost ukládá právní předpis nebo rozhodnutí orgánu veřejné moci. Příjemce důvěrné informace je povinen o takové skutečnosti bez zbytečného odkladu informovat poskytovatele důvěrné informace, nebrání-li mu v tom právní předpis nebo rozhodnutí orgánu veřejné moci. Příjemce důvěrné informace je v takovém případě oprávněn zpřístupnit pouze tu část Důvěrné informace, kterou je podle právního předpisu nebo rozhodnutí orgánu veřejné moci povinen zpřístupnit
3.5. Povinnost příjemce důvěrné informace zachovávat důvěrnost obchodního tajemství poskytovatele důvěrné informace a nevyužívat je, jakož i povinnost chránit osobní údaje fyzických osob, u nichž je povinnost ochrany či mlčenlivosti stanovena nařízením Evropského parlamentu a Rady (EU) 2016/679 (GDPR), zákonem č. 110/2019 Sb., o zpracování osobních údajů, nebo jinými obdobnými právními předpisy, trvá bez časového omezení i po ukončení spolupráce a vztahuje se na všechny zaměstnance a další osoby podílející se na plnění spolupráce.
3.6. Veškeré Důvěrné informace zůstávají ve vlastnictví poskytovatele důvěrné informace a žádné oprávnění či jiná práva vztahující se k těmto informacím nejsou udělena příjemci důvěrné informace nebo na něj převedena. Na žádost poskytovatele důvěrné informace je příjemce povinen neprodleně vrátit nebo zničit všechny nosiče Důvěrných informací, včetně kopií, které má k dispozici, s výjimkou částí obsažených v analýzách, studiích nebo jiných materiálech vytvořených příjemcem. I v takovém případě je příjemce povinen zachovávat jejich důvěrnost podle tohoto dokumentu.

4. Zpracování osobních údajů

4.1. Pokud příjemce důvěrné informace bude v souvislosti se spoluprací zpracovávat osobní údaje fyzických osob pro poskytovatele důvěrné informace, zavazuje se dodržovat veškeré povinnosti vyplývající z čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) a ze zákona č. 110/2019 Sb., o zpracování osobních údajů, zejména přijmout odpovídající technická a organizační opatření k zabezpečení ochrany osobních údajů.
4.2. Příjemce důvěrné informace omezí okruh osob, kterým budou osobní údaje zpřístupněny, pouze na osoby nezbytné pro plnění úkolů v rámci spolupráce, tyto osoby řádně poučí o jejich povinnostech podle právních předpisů o ochraně osobních údajů a zaváže je k mlčenlivosti o zpracovávaných osobních údajích.

5. Porušení povinností

5.1. V případě porušení povinnosti ochrany důvěrných informací podle tohoto dokumentu jednou ze stran, kterým druhé straně vznikne škoda, má poškozená strana právo na náhradu škody v souladu s občanským zákoníkem.
5.2. Strany se dohodly, že porušení povinnosti mlčenlivosti nebo ochrany důvěrných informací podle tohoto dokumentu zakládá povinnost uhradit druhé straně smluvní pokutu ve výši 200 000 Kč (slovy: dvě stě tisíc korun českých) za každý jednotlivý případ porušení. Smluvní pokuta je splatná do 15 dnů ode dne doručení písemné výzvy oprávněné strany. Zaplacením smluvní pokuty není dotčeno právo na náhradu škody v plném rozsahu.

6. Platnost a účinnost

6.1. Ustanovení o ochraně důvěrných informací obsažená v tomto dokumentu se sjednávají na dobu neurčitou.
6.2. Platnost těchto ustanovení může být ukončena písemným ujednáním stran, nejdříve však ke dni ukončení spolupráce nebo ke dni zániku smluv, které budou mezi stranami uzavřeny v souvislosti se spoluprací
6.3. Ukončením platnosti těchto ustanovení není dotčena účinnost těch povinností, které mají podle své povahy trvat i po ukončení spolupráce, zejména povinnost mlčenlivosti, ochrany obchodního tajemství a ochrany osobních údajů.
6.4. Tato ustanovení jsou závazná pro strany i pro jejich právní nástupce. Práva a povinnosti z nich vyplývající nelze převést na třetí osobu bez předchozího písemného souhlasu druhé strany

7. Závěrečná ustanovení

7.1. Tato ustanovení o ochraně důvěrných informací se řídí právním řádem České republiky. Není-li v tomto dokumentu stanoveno jinak, použijí se zejména příslušná ustanovení občanského zákoníku.
7.2. Veškerá oznámení podle tohoto dokumentu musí mít písemnou formu, musí být vyhotovena v českém jazyce a doručují se na adresy stran uvedené v záhlaví tohoto dokumentu, případně na jinou adresu, kterou jedna strana písemně oznámí druhé straně.
7.3. Strany se dohodly, že veškeré případné spory vzniklé v souvislosti s tímto dokumentem budou řešeny přednostně smírnou cestou. Spory, které se nepodaří vyřešit smírně, budou rozhodovány věcně příslušným soudem České republiky. Nestanoví-li právní předpis výlučnou místní příslušnost, je místně příslušným soudem obecný soud Jihočeského kraje.
7.4. Neplatnost některého ustanovení tohoto dokumentu nezakládá neplatnost ostatních ustanovení. V případě neplatnosti některého ustanovení se strany zavazují nahradit je ustanovením platným, které co nejvíce odpovídá jeho obsahu a účelu.
7.5. Tento dokument představuje úplné ujednání stran ve vztahu k předmětu ochrany důvěrných informací a nahrazuje veškerá předchozí ujednání, dohody, sdělení, přísliby nebo prohlášení učiněná mezi stranami, ať již v písemné nebo ústní formě.