SMLOUVA O POSKYTOVÁNÍ SLUŽEB

DNEŠNÍHO DNE, MĚSÍCE A ROKU:

Karlovarský kraj

se sídlem:	Závodní 353/88, 360 06 Karlovy Vary
zastoupený:	Mgr. Daniel Tovth, vedoucím odboru kancelář ředitelky úřadu na základě usnesení Rady Karlovarského kraje č. RK 1065/09/22 ze dne 19. 9. 2022 a čl. VII odst. 1 písm. d) podpisového řádu
IČO:	70891168
DIČ:	CZ70891168
bankovní spojení:	UniCredit Bank č.ú.: 1387678928/2700 Raiffeisenbank č.ú.: 7882138002/5500

*na straně jedné jako objednatel (dále jen „**objednatel**“)*

a

……

se sídlem:	……
zastoupený:	……
IČO:	……
DIČ:	……
bankovní spojení:	……
číslo účtu:	……

zapsaný v obchodním rejstříku ……

*na straně druhé jako poskytovatel (dále jen „**poskytovatel**“)*

(společně jako „smluvní strany“)

PREAMBULE

Vzhledem k tomu, že:

a) poskytovatel je vybraným dodavatelem z veřejné zakázky **„Provedení penetračních testů se zaměřením na bezpečnost informačních systémů Krajského úřadu Karlovarského kraje a Provedení auditu kybernetické bezpečnosti“** vyhlášené dne DD.MM.2025 objednatelem jako zadavatelem veřejné zakázky malého rozsahu; a
b) poskytovatel prohlašuje, že je držitelem potřebného živnostenského oprávnění a má řádné vybavení, zkušenosti a schopnosti, aby předmět smlouvy plnil ve stanovené době a ve sjednané kvalitě,

dohodly se smluvní strany na uzavření této

SMLOUVY

dle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

(dále jen „smlouva“)

I. Předmět smlouvy

1. 1 Předmětem této smlouvy je závazek poskytovatele:

1.1.1. provedení penetračních testů bez destruktivních dopadů na zařízení objednatele, kdy zhotovitel těchto penetračních testů není oprávněn v rámci testování vyřadit informační systém objednatele z provozu, ani není oprávněn v rámci testů k poškození SW nebo HW objednatele;

Externí penetrační test

Při realizaci bude prověřena bezpečnost a funkčnost prvků Krajského úřadu Karlovarského kraje, dostupných z veřejné sítě Internet. Tyto testy budou spočívat v simulaci útoku na systémy objednatele útočníkem, který se pokouší o průnik z prostředí internetu, nemá předběžné znalosti o IT infrastruktuře a nemá přístupové údaje k IT službám publikovaným z interního prostředí objednatele do internetu. Cílem testů je tedy prověření bezpečnosti veřejně dostupných systémů.

Testy z této skupiny budou obsahovat:

- vyhledání zranitelností v informacích veřejně dostupných o IT objednatele;
- bezpečnost DNS domény objednatele, zejména pak počet, umístění a dostupnost DNS obsahu serverů, možnost neautorizovaného transferu zóny a zabezpečení proti neoprávněné změně DNS záznamů;
- bezpečnost infrastruktury elektronické pošty objednatele, zejména pak ochrana pošty odesílané z domény objednatele, ochrana pošty pro doménu objednatele – účinnost antispamu a antiviru, prozrazení zneužitelných informací prostřednictvím protokolů a rozhraní použitých pro elektronickou poštu (zhotovitel nebude cílit na prozrazení obsahu zpráv elektronické pošty zaměstnanců objednatele, nýbrž na informace obsažené v hlavičkách – předmětu e-mailů, formulářů apod. a posouzení zabezpečení odesílání pošty z webu objednatele (z formulářů na webu objednatele);
- bezpečnost vybraných služeb, portálů a informačních systémů publikovaných do internetu, tj. veškeré weby.

Způsob realizace

Bude se jednat o nekooperativní externí penetrační testy, které se budou skládat z:

- prvotního skenu systému, po kterém budou následovat cílený test systému, které v rámci skenu vykazují chybu; cílený test proběhne se znalostí přístupových údajů,
- testů webových aplikací z pohledu běžného uživatele aplikace – testování se znalostí přístupových údajů,
- testů k získání informací, identifikace funkčních systémů,
- všeobecných testů zranitelnosti,
- testů týkajících se charakteristiky infrastruktury systému,
- testů spolehlivosti konfigurace,
- testů existence backdoors (detekce otevřených míst v systému),
- testů autentizace a schémat pro kontrolu přístupu,
- testů firewallů,
- testů routerů,
- kontroly operačních systémů,
- testů aplikačních chyb a vad v systému a
- testů nedostatečného provozního zabezpečení.

Interní penetrační test

Interní penetrační testy budou prováděny z prostředí interní LAN sítě zadavatele. Zaměří se na test používané infrastruktury a zabezpečení bezdrátové sítě bez a se znalostí hesla. Součástí je i pokročilá detekce na odhalení známých či neznámých hrozeb vyskytujících se již v síti objednatele (pokročilý malware, ransomware, apod.). Jejich cílem je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu interní sítě, resp. jeho možné ohrožení z prostředí interní sítě a bezdrátové sítě a testování bezdrátové sítě samotné, tj. bude tedy proveden řízený útok na infrastrukturu zadavatele z vnitřní interní sítě, tj. bude simulováno počínání potencionálního útočníka pokoušejícího se o průnik z nakaženého počítače umístěného uvnitř interní sítě.

Interní penetrační testy budou částečně kopírovat externí testy pro interní datovou síť a dále budou zaměřeny na realizaci:

- testů k získání informací, identifikace funkčních systémů,
- všeobecných testů zranitelnosti,
- testů týkajících se charakteristiky infrastruktury systému,
- testů spolehlivosti konfigurace,
- testů existence backdoors (detekce otevřených míst v systému),
- testů autentizace a schémat pro kontrolu přístupu,
- kontroly operačních systémů,
- testů aplikačních chyb a vad v systému,
- testů nedostatečného provozního zabezpečení,
- testování slabých míst zahrnující body selhání, s cílem způsobit odmítnutí služeb webových aplikací,
- odposlech komunikace se systémem,
- odchycení a přesměrování této komunikace,
- zneužití odchycených informací a komunikace směrem k aplikačním službám (serverům), - útoky na uživatele systému prostřednictvím tohoto systému a
- testů wi-fi bodů přístupu.

Penetrační test s využitím sociotechnických metod

V rámci tohoto testu je požadováno prověření dodržování procesů a bezpečnostních zásad v rámci Krajského úřadu Karlovarského kraje, a to ve třech etapách:

- *Phishingový test formou „podvodného“ e-mailu*

Cílem testování je prověřit úroveň bezpečnostního povědomí zaměstnanců a přinutit uživatele sdělit citlivé informace nebo vykonat určitou činnost.
Proběhne phishingová kampaň s podvrženými e-maily s cílem otestování uživatelských účtů (uživatelů) a to v podobě podvrženého e-mailu. Během testu nedojde k infikování koncových bodů, ale bude zaznamenána a změřena aktivní odezva na e-mail – „proklik“ na odkaz v e-mailu.

- *Test formou nastražených USB flash disků*

Cílem testu je prověřit úroveň bezpečnostního povědomí zaměstnanců a přinutit uživatele vložit nalezený USB flash disk do PC a pokusit se zjistit co daný disk obsahuje.

- *Test fyzické bezpečnosti*

Cílem testu je pokus o proniknutí neautorizované osoby do vnitřních prostor Krajského úřadu Karlovarského kraje a zde získat přístup k prostředkům informačního systému nebo citlivým informacím.

Výsledky testování a výsledná zpráva

Výstupem penetračního testování bude závěrečná zpráva, která v přehledné podobě (číselné, grafické i slovní vyjádření) shrne a popíše všechny výše vyjmenované provedené penetrační testy vč. zranitelností, stupně rizikovosti a návrhu opatření, která povedou k jejich odstranění nebo zmírnění rizika spojeného s těmito zranitelnostmi na přijatelnou úroveň. Zpráva bude předána v tištěné podobě – 1 pare a dále pak v elektronické podobě prostřednictvím elektronického uložiště, dle následné domluvy. Závěrečná zpráva bude obsahovat tyto části:

a) Manažerské shrnutí – přehledně prezentované penetrační testy a celkové zhodnocení bezpečnosti systému.
b) Popis postupů či metodiky provedených penetračních testů, zvlášť pro externí penetrační test, interní penetrační test a penetrační test za použití sociotechnických metod.
c) Log Book – přehled provedených prací, popis jednotlivých provedených testů. Dalším výstupem budou logy provedených testů z použitých bezpečnostních aplikací, které budou sloužit k ověření provedení jednotlivých testů dle checklistu OWASP – seznamu první desítky nejzávažnějších bezpečnostních rizik webových aplikací.
d) Popis nalezených zranitelností – detailní popis jednotlivých nalezených zranitelností včetně stupně rizikovosti a jejich dopadu na testovanou aplikaci. U nalezených zranitelností bude součástí zprávy i kód (ideálně http, dotaz a odpověď), který umožňuje replikaci testu objednavatelem.
   Rizikovost bude rozdělena dle následujících kritérií: d1) kritické – zranitelnost vedoucí k okamžitému a naprostému vyřazení služby; d2) vysoké – zranitelnosti, které v kombinaci s jinými zranitelnostmi představují zásadní vysoké riziko; d3) střední – musejí být splněny speciální podmínky na zneužití uvedených zranitelností nebo jejich případné zneužití má omezený dopad; d4) nízké – drobné bezpečnostní problémy.
e) Navrhované opatření – popis navrhovaných opatření k jednotlivým identifikovaným zranitelnostem, která povedou k odstranění nalezených zranitelností nebo ke snížení míry rizika spojeného s těmito zranitelnostmi na akceptovatelnou úroveň.
f) Závěrečné shrnutí – shrnuje provedené externí a interní penetrační testy a penetrační testy s využitím sociotechnických metod a obsahuje celkové hodnocení úrovně bezpečnosti informačních systémů objednatele.

1.1.2 provedení pravidelného auditu kybernetické bezpečnosti Krajského úřadu Karlovarského kraje, a to kvalifikovaným auditorem provádějícím pravidelný i finální bezpečnostní audit (jméno a příjmení, titul).

Součástí auditu kybernetické bezpečnosti bude posouzení souladu s legislativními požadavky v oblasti informační bezpečnosti, které jsou relevantní pro Karlovarský kraj. Jedná se zejména o § 16 odst. 2) písm. b) vyhláška o kybernetické bezpečnosti. Rozsah auditu bude zahrnovat všechna nezbytná organizační i technická opatření uvedená v § 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů a bude proveden v souladu s požadavky tohoto zákona a zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti.

Výstupem z této fáze bude:

- **Závěrečná zpráva z auditu kybernetické bezpečnosti** – dokument bude obsahovat všechny náležitosti požadované vyhláškou o kybernetické bezpečnosti, zejm.:
- cíle auditu kybernetické bezpečnosti,
- předmět auditu kybernetické bezpečnosti,
- kritéria auditu kybernetické bezpečnosti,
- identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily,

- datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti,
- zjištění z auditu kybernetické bezpečnosti (identifikované nedostatky vůči legislativním požadavkům),
- závěry auditu kybernetické bezpečnosti.
- **Seznam nápravných opatření**, které je potřeba vykonat.

Závěrečná zpráva bude předána v tištěné podobě – 1 paré a dále pak v elektronické podobě prostřednictvím elektronického uložiště, dle následné domluvy.

Činnosti dle odst. 1.1.1 a 1.1.2 jsou dále uvedeny také jako „Služby“.

1. 2 Objednatel se zavazuje zaplatit poskytovateli za řádné provedení penetračních testů a pravidelného auditu kybernetické bezpečnosti cenu ve výši a způsobem uvedeným v čl. III. této smlouvy, a to bezhotovostním převodem na bankovní účet poskytovatele, uvedený v záhlaví této smlouvy.

1. 3 Přístup do systému v rámci smluveného penetračního testování nebude vnímán jako kybernetický bezpečnostní incident dle zákona o kybernetické bezpečnosti nebo porušení zabezpečení osobních údajů dle čl. 33 GDPR.

1. 4 Poskytovatel provede testy výhradně nedestruktivními metodami a s maximální snahou zamezit negativnímu dopadu na dostupnost, integritu a důvěrnost.

1. 5 Výslovně se zakazuje provádět volumetrické testy dostupnosti, destruktivní payloady, fuzzing proti produkčním databázím, bruteforce vedoucí k lockoutům, testy mimo schválená okna a testy proti třetím stranám bez jejich písemného souhlasu.

1. 6 Testy budou probíhat pouze v oknech, která budou specifikována při koordinační schůzce po podpisu smlouvy. Objednatel může test kdykoli zastavit vyhlášením „STOP“ a poskytovatel okamžitě přeruší veškeré aktivity.

1. 7 Poskytovatel odpovídá za škodu způsobenou porušením smlouvy nebo nedbalým či úmyslně chybným postupem. Pokud k dopadu (ohrožení, omezení či nefunkčnost testovaných informačních systémů) dojde i při dodržení doporučených standardů pro provádění penetračních testů, jako je např. metodika OSSTMM a standardy NIST 800-11 a další a dohodnutých limitů, odpovědnost nebude na straně poskytovatele těchto testů.

1. 8 Poskytovatel nejpozději do 10 pracovních dnů odstraní veškeré zanechané artefakty (účty, klíče, agenti apod.) a předá jejich seznam objednateli. Po nápravě kritických nálezů bude proveden bezplatně jeden retest v rozsahu nápravy.

II. Termín a místo plnění

2.1 Poskytovatel je povinen provést Služby a předat závěrečné zprávy v termínu do 90 kalendářních dnů od účinnosti smlouvy.

2.2 Místem provedení Služby a předání závěrečných zpráv je sídlo objednatele

III. Cena a platební podmínky

3.1 Cena za provedení penetračních testů dle článku 1.1.1 smlouvy činí:

cena bez DPH	0,00 Kč (slovy: …… korun českých)
DPH	0,00 Kč (slovy: …… korun českých)
cena včetně DPH	0,00 Kč (slovy: …… korun českých)

3.2 Cena za audit kybernetické bezpečnosti dle článku 1.1.2 smlouvy činí:

cena bez DPH	0,00 Kč	(slovy: ..... korun českých)
DPH	0,00 Kč	(slovy: ..... korun českých)
cena včetně DPH	0,00 Kč	(slovy: ..... korun českých)

3.3 **Cena celkem** za provedení penetračních testů dle čl. 1.1.1 a auditu kybernetické bezpečnosti dle článku 1.1.2 smlouvy činí:

cena bez DPH	0,00 Kč	(slovy: ..... korun českých)
DPH	0,00 Kč	(slovy: ..... korun českých)
cena včetně DPH	0,00 Kč	(slovy: ..... korun českých)

3.4 Smluvní strany se dohodly, že cena dle předchozího odstavce zahrnuje veškeré náklady poskytovatele vynaložené poskytovatelem za plnění Služeb. Cena nebude předmětem zvýšení, pokud tato smlouva výslovně nestanoví jinak.

3.5 Daň z přidané hodnoty bude připočtena k ceně ve výši dle právní úpravy účinné ke dni uskutečnění zdanitelného plnění.

3.6 Cenu za provedení penetračních testů a auditu uhradí objednatel na základě faktur vystavené poskytovatelem dle čl. III. odst. 3.3 smlouvy po provedení všech Služeb a předání závěrečné zprávy penetračního testování a závěrečné zprávy z auditu kybernetické bezpečnosti objednateli.

3.7 Faktura bude obsahovat náležitosti daňového dokladu stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „ZDPH“) a zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. V případě, že faktura nebude obsahovat správné údaje či bude neúplná, je objednatel oprávněn fakturu vrátit ve lhůtě do data její splatnosti poskytovateli. Poskytovatel je povinen takovou fakturu opravit, aby splňovala podmínky stanovené v tomto odstavci tohoto článku smlouvy. Lhůta splatnosti běží u opravené faktury od začátku.

3.8 Splatnost faktury je smluvními stranami dohodnuta na třicet (30) kalendářních dnů ode dne řádného doručení faktury objednateli. Za den úhrady faktury bude považován den odepsání fakturované částky z účtu objednatele.

3.9 Smluvní strany této smlouvy se dohodly, že poskytovatel, coby poskytovatel zdanitelného plnění, je povinen bez zbytečného prodlení písemně informovat objednatele o tom, že se stal nespolehlivým plátcem ve smyslu ustanovení § 106a ZDPH. Smluvní strany si dále společně ujednaly, že pokud objednatel v průběhu platnosti tohoto smluvního vztahu na základě informace od poskytovatele či na základě vlastního šetření zjistí, že se poskytovatel stal nespolehlivým plátcem ve smyslu § 106a ZDPH, souhlasí obě smluvní strany s tím, že objednatel uhradí za poskytovatele daň z přidané hodnoty z takového zdanitelného plnění dobrovolně správci daně dle § 109a citovaného právního předpisu. Zaplacení částky ve výši daně objednatelem správci daně pak bude smluvními stranami považováno za splnění závazku uhradit sjednanou cenu, resp. její část. Smluvní strany si v této souvislosti poskytnou veškerou nezbytnou součinnost při vzájemném poskytování informací požadovaných ZDPH. Poskytovatel současně souhlasí s tím, že je povinen objednateli nahradit veškerou škodu vzniklou v důsledku portálu institutu ručení ze strany správce daně. Smluvní strany se dohodly, že objednatel bude hradit sjednanou cenu pouze na účet zaregistrovaný a zveřejněný ve smyslu § 96 odst. 1 ZDPH.

IV. Mlčenlivost

4.1 Poskytovatel i objednatel mají povinnost mlčenlivosti ohledně všech skutečností, s nimiž se seznámili v souvislosti s plněním této smlouvy. Poskytovatel i objednatel se zavazují zajistit, aby veškeré osoby, jež se budou podílet na plnění smlouvy, byly zavázány mlčenlivostí.

4.2 Povinnost mlčenlivosti dle této smlouvy se vztahuje i na všechny třetí osoby, které budou poskytovat Podporu dle této smlouvy. Odpovědnost za porušení mlčenlivosti třetí osobou nese poskytovatel.

4.3 Povinnost mlčenlivosti se nevztahuje na případy, kdy je zpřístupnění určitých informací vyžadováno právními předpisy.

V. Smluvní pokuta

5.1 Smluvní strany se dohodly, že v případě prodlení poskytovatele s plněním Služeb dle čl. II odst. 2.1 této smlouvy, je objednatel vůči němu oprávněn uplatnit smluvní pokutu ve výši 0,1 % z ceny dle čl. III. odst. 3.3 smlouvy včetně DPH, a to za každý i započatý den prodlení.

5.2 Smluvní strany se dohodly, že v případě, kdy objednatel neuhradí bez zjevného důvodu cenu plnění do data splatnosti, je poskytovatel vůči němu oprávněn uplatnit smluvní pokutu ve výši 0,1 % z dlužné částky, a to za každý i započatý den prodlení.

5.3 Smluvní strany se dohodly, že v případě porušení mlčenlivosti dle čl. IV. poskytovatelem nebo třetí osobou, je objednatel oprávněn vůči němu uplatnit smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každé porušení.

5.4 Smluvní strany se dohodly, že v případě že dojde k omezení provozu či funkčnosti testovaných informačních systémů, které byly způsobeny nedbalým postupem či porušením smlouvy, je objednatel oprávněn vůči poskytovateli uplatnit smluvní pokutu ve výši:

a) Kritické systémy (portály pro veřejnost, podatelna, platební brány) 30.000, - Kč/každá započatá hodina

b) Vysoká důležitost (klíčové interní IS, identity, síťové prvky) 15.000, - Kč//každá započatá hodina

c) Střední důležitost (podpůrné IS): 6.000, - Kč /každá započatá hodina.

Maximální pokuta činí 250.000,- Kč/incident.

5.5 Smluvní pokuta je splatná do třiceti dní od data, kdy byla povinné straně doručena písemná výzva k jejímu zaplacení oprávněnou stranou, a to na účet oprávněné strany uvedený v písemné výzvě.

5.6 Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši.

VI. Ukončení smlouvy

6.1 Smluvní strany se dohodly, že mohou od této smlouvy odstoupit v případech, kdy tak stanoví zákon, jinak v případě podstatného porušení této smlouvy. Odstoupení od smlouvy musí být provedeno písemnou formou a je účinné okamžikem jeho doručení druhé smluvní straně. Odstoupením od smlouvy se tato smlouva ruší od okamžiku doručení projevu vůle směřujícího k odstoupení od smlouvy druhé smluvní straně.

6.2 Za podstatné porušení smlouvy poskytovatelem se považuje:

a) prodlení poskytovatele s provedením penetračních testů a auditu kybernetické bezpečnosti, dle čl. II. odst. 2.1 smlouvy o více než 10 kalendářních dní;

b) je proti němu zahájeno insolvenční řízení;

c) vstoupí do likvidace;

6.3 Za podstatné porušení smlouvy objednatelem se považuje:

a) prodlení s úhradou ceny plnění po dobu delší než 30 kalendářních dnů, pokud objednatel neuhradí poskytovateli dlužnou částku ani v náhradní lhůtě poskytnuté poskytovatelem objednateli v písemné výzvě.

VII. Komunikace smluvních stran

8.1 Kontaktní osobou za objednatele ve věcech plnění předmětu smlouvy je:

……

8.2 Kontaktní osobou za poskytovatele ve věcech plnění předmětu smlouvy je:

……

8.3 Veškerá podání a jiná oznámení, která se doručují smluvním stranám, je třeba doručit osobně, nebo doporučenou listovní zásilkou s doručenkou nebo datovou schránkou, pokud není ve smlouvě stanoveno jinak.

8.4 Aniž by tím byly dotčeny další prostředky, kterými lze prokázat doručení, má se za to, že oznámení bylo řádně doručené:

a) při doručování osobně:

- dnem faktického přijetí oznámení příjemcem; nebo
- dnem, v němž bylo doručeno osobě na příjemcově adrese určené k přebírání listovních zásilek; nebo
- dnem, kdy bylo doručováno osobě na příjemcově adrese určené k přebírání listovních zásilek, a tato osoba odmítla listovní zásilku převzít; nebo
- dnem, kdy příjemce při prvním pokusu o doručení zásilku z jakýchkoli důvodů nepřevzal či odmítl zásilku převzít, a to i přesto, že se v místě doručení nezdržuje, pokud byla na zásilce uvedena adresa pro doručování ze záhlaví smlouvy.

b) při doručování prostřednictvím držitele poštovní licence:

- dnem předání listovní zásilky příjemci; nebo
- dnem, kdy příjemce při prvním pokusu o doručení zásilku z jakýchkoli důvodů nepřevzal či odmítl zásilku převzít, a to i přesto, že se v místě doručení nezdržuje, pokud byla na zásilce uvedena adresa pro doručování ze záhlaví smlouvy.

c) při doručování do datové schránky:

- dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

VIII. Závěrečná ustanovení

9.1 Poskytovatel bere na vědomí, že objednatel je povinen uveřejnit tuto smlouvu ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

9.2 Zaslání smlouvy do registru smluv zajistí objednatel neprodleně po podpisu smlouvy. Objednatel se současně zavazuje informovat poskytovatele o provedení registrace tak, že zašle poskytovateli kopii potvrzení správce registru smluv o uveřejnění smlouvy bez zbytečného odkladu poté, kdy sám potvrzení obdrží, popř. již v průvodním formuláři vyplní příslušnou kolonku

s ID datové schránky poskytovatele (v takovém případě potvrzení od správce registru smluv o provedení registrace smlouvy obdrží obě smluvní strany zároveň).

9.3 Smluvní strany této smlouvy se dohodly, že právní vztahy založené touto smlouvou se budou řídit právním řádem České republiky. Tato smlouva jakož i právní vztahy touto smlouvou neupravené se řídí úpravou zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“).

9.4 Případné spory vzniklé z této smlouvy budou řešeny dohodou smluvních stran a nebude-li dohody, pak podle platné právní úpravy věcně a místně příslušnými soudy České republiky.

9.5 V případě neplatnosti nebo neúčinnosti některého ustanovení této smlouvy nebudou dotčena ostatní ustanovení této smlouvy.

9.6 Smluvní strany prohlašují, že skutečnosti uvedené v této smlouvě nepovažují za obchodní tajemství ve smyslu ustanovení § 504 občanského zákoníku.

9.7 Poskytovatel je povinen spolupůsobit při výkonu finanční kontroly ve smyslu § 2 písm. e) a § 13 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, tj. poskytnout kontrolnímu orgánu doklady o dodávkách zboží a služeb hrazených z veřejných výdajů nebo z veřejné finanční podpory v rozsahu nezbytném pro ověření příslušné operace. Tutéž povinnost bude poskytovatel povinen požadovat po svých dodavatelích.

9.8 Tuto smlouvu lze měnit, doplňovat a upřesňovat pouze oboustranně odsouhlasenými, písemnými a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou smluvních stran, které musí být obsaženy na jedné listině.

9.9 Smlouva je vyhotovena ve třech stejnopisech, z nichž objednatel obdrží dva výtisky a poskytovatel jeden výtisk. Každý stejnopis této smlouvy má právní sílu originálu.

Nebo alternativně (při podpisu se ponechá relevantní alternativa):

Tato smlouva je uzavřena elektronicky.

9.10 Tato smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem uveřejnění v registru smluv.

9.11 Obě smluvní strany potvrzují autentičnost této smlouvy a prohlašují, že si smlouvu včetně příloh přečetly, s jejím obsahem (včetně příloh) souhlasí, že smlouva byla sepsána na základě pravdivých údajů, z jejich pravé a svobodné vůle a nebyla uzavřena v tísni ani za jinak jednostranně nevýhodných podmínek, což stvrzují svým podpisem, resp. podpisem svého oprávněného zástupce.

V ……dne…… V ……dne……

_____ _____

……
……

Mgr. Daniel Tovth
vedoucí odboru
kancelář ředitelky úřadu
Karlovarský kraj