DODATEK Č. 1 KE Smlouvě o poskytování ÚDRŽBY A KOMPLEXNÍ PROVOZNÍ podpory TRŽIŠŤ DATOVÉHO SKLADU ZLÍNSKÉHO KRAJE

Uzavřený dle § 2586 a násl. a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

mezi:

**Zlínský kraj**

se sídlem: třída Tomáše Bati 21, 761 90 Zlín

zastoupená: Ing. Radim Holiš, hejtman

IČO: 70891320

DIČ: CZ70891320

bankovní spojení: Česká spořitelna, a.s., č. ú.: 2786182/0800

datová schránka: scsbwku

(dále jen „Objednatel“)

a

GIST Consulting, s.r.o.

se sídlem: Collinova 421, 500 03 Hradec Králové  
zastoupená: Ing. Romanem Šatalíkem, jednatelem

IČO: 19642041

DIČ: CZ19642041

bankovní spojení: Komerční banka a.s., č.ú. 131-1198050277/0100

datová schránka: hjn4sbw

zapsaný v OR: u KS Hradec Králové, odd. C, vložka 51683

(dále jen „Poskytovatel“)

1. **Úvodní ustanovení**
   1. Objednatel uzavřel dne 29. 6. 2020 s Poskytovatelem Smlouvu o poskytování údržby a komplexní provozní podpory tržišť datového skladu Zlínského kraje č. smlouvy Objednatele D/3418/2020/KŘ-IT, č. smlouvy Poskytovatele 04/26/2020 (dále jen „Smlouva“). Smlouvou byla stanovena cena, která byla uvedená v příloze č. 2 Smlouvy. Tato cena byla od uzavření Smlouvy do doby uzavření tohoto dodatku navýšena podle meziročního nárustu inflace vyhlášeného ČSÚ na částku uvedenou v příloze č. 1 tohoto dodatku.
   2. Původní smluvní stranou Smlouvy byla společnost GIST, s.r.o. V důsledku rozdělení obchodní společnosti GIST, s.r.o., se sídlem Collinova 421, Věkoše, 500 03 Hradec Králové, IČO 60916851, jako rozdělované společnosti, formou odštěpení se vznikem nové obchodní společnosti došlo s účinností ke dni zápisu této přeměny do obchodního rejstříku k odštěpení části jmění rozdělované společnosti a jeho přechodu na nově vznikající společnost, kterou je obchodní společnost GIST Consulting, s.r.o., se sídlem Hradec Králové, Collinova 421, PSČ 500 03, a to v souladu s příslušným projektem rozdělení. Na tuto nově vzniklou společnost přešel i závazek ze Smlouvy.
   3. Smluvní strany se dodatkem dohodly na prodloužení platnosti této smlouvy, a to do 30. 6. 2028.
2. **Změny smlouvy**
   1. Článek 4.7 Smlouvy se mění a nově zní

Veškeré daňové doklady (faktury) vystavené Poskytovatelem podle této Smlouvy bude Poskytovatel v jednom vyhotovení zasílat Objednateli přednostně do jeho datové schránky nebo na email *fakturace@zlinskykraj.cz* a jejich splatnost bude činit třicet (30) kalendářních dní ode dne jejich doručení Objednateli. Za den úhrady dané faktury bude považován den odepsání fakturované částky z účtu Objednatele.

* 1. Článek 10.1 Smlouvy se mění a nově zní

Tato smlouva se uzavírá na dobu určitou, a to od 1. 7. 2020 do 30. 6. 2028.

* 1. Původní Příloha č. 3 Smlouvy s názvem „Bezpečnostní pravidla ICT Zlínského kraje“ se nahrazuje Přílohou č. 2 tohoto dodatku s názvem „Bezpečnostní pravidla ICT Zlínského kraje“.
  2. Článek 9.7 smlouvy se mění a nově zní

Za porušení povinností týkajících se ochrany obchodního tajemství, důvěrných informací podle článku 7 nebo osobních údajů podle článku 13 nebo auditu článku 14 nebo bezpečnostních pravidel dle článku 12 této Smlouvy a přílohy 3 této Smlouvy - článku 14 má poškozená smluvní strana právo uplatnit u druhé Smluvní strany, která tyto povinnosti porušila, nárok na zaplacení smluvní pokuty ve výši 10.000,- Kč za každý zjištěný případ porušení.

1. **Závěrečná ustanovení**
   1. Tento dodatek nabývá platnosti podpisem obou smluvních stran a účinnosti dnem zveřejnění v registru smluv dle 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. Smluvní strany se dohodly, že Objednatel v zákonné lhůtě odešle tento dodatek k řádnému uveřejnění do registru smluv vedeného Ministerstvem vnitra ČR. O uveřejnění tohoto dodatku Objednatel bezodkladně informuje Poskytovatele (postačí e-mailem prostřednictvím kontaktní osoby/osoby oprávněné jednat ve věcech technických nebo smluvních).
   2. Ostatní ustanovení Smlouvy tímto dodatkem nedotčená se nemění a zůstávají nadále v platnosti.
   3. Příloha tohoto dodatku je jeho nedílnou součástí. Přílohou tohoto dodatku je:

Příloha č. 1 tohoto dodatku – Cena za komplexní provozní podporu

Příloha č. 2 tohoto dodatku – Bezpečnostní pravidla ICT Zlínského kraje

* 1. Tento dodatek je vyhotoven elektronicky a podepsán uznávanými, resp. kvalifikovanými elektronickými podpisy oprávněných osob. Za datum podpisu se považuje údaj uvedený v časovém razítku, pokud není, pak datum uvedené v elektronickém podpisu podepisující strany.
  2. Účastníci tohoto dodatku prohlašují, že dodatek uzavřeli po zralé úvaze, svobodně a vážně, nikým a ničím k tomu nenuceni. Zároveň prohlašují, že se detailně seznámili s textem dodatku, že rozumějí užívaným pojmům a že k textu dodatku nemají žádných výhrad.

**Doložka dle § 23 zákona č. 129/2000 Sb., o krajích, ve znění pozdějších předpisů**

Rozhodnuto orgánem kraje: Rada Zlínského kraje

Datum: 25. 3. 2024 usnesení č. 0304/R08/24

Zkontroloval:

Ve Zlíně dne: V Hradci Králové dne:

za Objednatele za Poskytovatele

......................................................................

Ing. Radim Holiš Roman Šatalík

hejtman jednatel společnosti

**Příloha č. 1 – Cena za komplexní provozní podporu**

1. **Cena** 
   1. **Základní komplexní podporA**

Cena bez DPH /rok 126 558,00 Kč

DPH 26 577,00 Kč

**Cena včetně DPH /rok 153 135,00 Kč**

(slovy sto padesát tři sto třicet pět korun padesát haléřů českých).

Výše čtvrtletní komplexní podpory činí jednu čtvrtinu celkové ceny bez DPH.

* 1. **Rozšířená podpora - činnosti nad rámec komplexní podpory**

Jednotkové ceny služeb:

**Hodinová sazba činností Cena bez DPH**

Operátorské, programátorské práce…………………………………… 1 980,00 Kč

Analytické práce, odborné konzultace, konfigurace systému………. 1 980,00 Kč

Školení uživatelů do 10 osob…………………………………………… 1 319,00 Kč

Při činnostech prováděných u Objednatele mimo sídlo firmy GIST, spol. s r.o. (pracoviště Hradec Králové, Collinova 421) v rámci služeb rozšířené podpory budou účtovány cestovní náklady, které zahrnují náklady na dopravu osobním automobilem za cenu 10,60 Kč /km bez DPH, DPH 2,20 Kč a cena celkem včetně DPH 12,80 Kč.

**Příloha č. 2** - **Bezpečnostní pravidla ICT Zlínského kraje**

Verze 2.5

**ICT** (informační a komunikační technologie) jsou veškeré informační technologie používané pro komunikaci a práci s informacemi

**IS** (Informační systém) je celek složený z počítačového hardwaru, souvisejícího softwaru a dat.

**Správce IS** je pracovník Odboru informačních a komunikačních technologií, Oddělení serverové a síťové infrastruktury ZK. Je uveden jako odpovědná osoba předávajícího v předávacím protokolu o předání přihlašovacích údajů.

**Druhá smluvní strana** je subjekt, se kterým Zlínský kraj uzavřel smlouvu, jejíž přílohou jsou tato bezpečnostní pravidla, a dále všichni jeho pracovníci, poddodavatelé apod.

**Při porušení bezpečnostních pravidel druhou smluvní stranou mohou být přidělené přístupové účty bez předchozího upozornění zablokovány nebo zcela odebrány.**

1. **Přístup k IS ZK**
   1. Přístup jiných subjektů (druhé smluvní strany) k IS ZK je možný pouze na základě smluvně ošetřeného vztahu se Zlínským krajem.
   2. Druhá smluvní strana je povinna používat pouze jí přidělené přístupy a povolené způsoby přístupu, (fyzické přístupy, přístupové údaje, povolené časy pro přístup a přidělená oprávnění), a je odpovědná za jejich používání. Přidělené údaje jsou pro druhou stranu závazné, jsou důvěrné a jsou platné jen po dobu platnosti smlouvy. Tyto údaje jsou uvedeny v Předávacím protokolu k účtu. Přidělené přístupové údaje jsou přiděleny konkrétní osobě a nesmí být sdíleny.
   3. Přístupy a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků. Druhá smluvní strana nesmí bez souhlasu správce IS vytvářet nové přístupové účty a do přidělených účtů a oprávnění zasahovat a měnit je. Pokud druhá smluvní strana zjistí, že skutečná oprávnění jsou odlišná od dohodnutých, neprodleně na to upozorní odpovědné osoby nebo Správce IS.
   4. Přistupovat k IS ZK mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením prací poučení a proškolení všech svých pracovníků a subdodavatelů, kteří budou přistupovat k IS ZK.
2. **Práce v IS ZK**
   1. Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla a stanovené postupy pro práci v IS ZK a nese v souladu s platnou legislativou a předpisy svůj díl odpovědnosti za nedodržení či porušení pravidel, případně za škody vzniklé v důsledku bezpečnostních incidentů, které zavinila.
   2. Druhá smluvní strana zajistí přiměřenou úroveň bezpečnostního povědomí svých zaměstnanců a dodavatelů, kteří se podílejí na plnění předmětu smlouvy.
   3. Je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům. Dále je zakázáno provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, monitorování síťové komunikace, dostupnosti síťových prostředků a služeb a způsobů zabezpečení které nesouvisí s plněním předmětu smlouvy, a provádět pokusy o jejich překonání.
   4. Druhá smluvní strana nesmí vytvářet žádné přístupové cesty do IS ZK a měnit přístupová oprávnění. Tyto změny může provádět Správce IS na základě písemné žádosti.
   5. Činnost druhé smluvní strany v IS ZK je monitorována a evidována. Neoprávněné aktivity může Správce IS zakázat. Pověření pracovníci ZK mohou ověřovat dodržování stanovených bezpečnostních pravidel a plnění smluvních povinností, nebo je nechat prověřit třetí stranou. Druhá smluvní strana jim při tom poskytne nezbytnou součinnost. V případě zjištění nedostatků je povinna druhá smluvní strana tyto odstranit ve lhůtě stanovené Správcem IS.
   6. Pracovníci druhé smluvní strany jsou povinni řídit se pokyny odpovědných osob (uvedených ve smlouvě), Správců IS a dalších pracovníků Odboru informačních a komunikačních technologií.
   7. Druhá smluvní strana je povinna bez zbytečného prodlení předávat Správci IS informace o provedených zásazích a změnách, promítnout je do dokumentace a předat Správci IS. Všechny změny, které mohou ovlivnit bezpečnost IS ZK, musí být předem projednány a schváleny Správcem IS.
3. **Účty a hesla**
   1. Druhá smluvní strana je povinna chránit přístupové účty heslem. Druhá strana nesmí sdělit názvy účtů a hesla žádné neoprávněné osobě. Heslo musí splňovat aktuální požadavky ZK na kvalitu a platnost a musí být uchováno v tajnosti. Hesla musí být vždy předávána bezpečným způsobem. Pokud je to možné, musí být použita více faktorová autentizace.
   2. Přístupové účty jsou standardně neaktivní. Jejich aktivaci schvalují a zajištují na základě žádosti druhé smluvní strany odpovědné osoby ZK. Žádost musí obsahovat informace o prováděných činnostech a předpokládané době prací. Druhá smluvní strana nesmí bez předchozího schválení provádět jiné než nahlášené práce.
4. **Vzdálený přístup a vzdálená údržba**
   1. Vzdálený přístup do IS ZK je možný pouze dohodnutým způsobem, popsaným ve smlouvě nebo schválené technické dokumentaci. Vzdálený přístup musí být vždy šifrován.
   2. Druhá smluvní strana smí vzdáleně přistupovat do IS ZK pouze z pracovní stanice, která má nainstalovaný podporovaný operační systém, nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem, a má aktivní a aktuální antivirovou ochranu.
   3. Druhá smluvní strana smí vzdáleně přistupovat do IS ZK pouze z ověřených IP adres. Konkrétní IP adresy schvaluje Správce IS.
   4. Přístup k systémům v oblastech s vysokou úrovní zabezpečení za účelem vzdálené údržby (např. u významných informačních systémů ZK) musí být chráněn kromě šifrování i silnou autentizací druhé smluvní strany.
   5. Pracovní stanice určené k přístupu do IS ZK ze vzdálené lokality musí být druhou smluvní stranou fyzicky zabezpečeny proti přístupu neoprávněných osob.
5. **Zabezpečení fyzického přístupu k IS**
   1. Servery, síťové komponenty a další ICT zařízení jsou zabezpečeny proti fyzickému přístupu. Přístup do místností se servery s citlivými daty a přístup k síťovým zařízením je regulován a odpovídajícím způsobem monitorován. Pokud fyzické zabezpečení citlivých dat není dostatečné, musí být zabezpečena šifrováním.
   2. Opravy ICT komponent mohou být prováděny pouze na základě smluvně ošetřeného vztahu se ZK.
   3. Fyzický přístup k prostředkům IS je umožněn pouze druhým smluvním stranám (servisní a dodavatelské organizace, dohody o provedení práce apod.), u kterých udělení přístupu vyplývá z uzavřené smlouvy. Fyzický přístup k prostředkům IS je možné uskutečnit pouze se souhlasem Správce IS nebo vedoucího oddělení serverové a síťové infrastruktury, Odboru informačních a komunikačních technologií.
   4. Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků Odboru informačních a komunikačních technologií nebo jimi pověřených osob.
   5. Pro přímé připojení (v prostorách ZK) do IS ZK smí být použita pouze přidělená technika ZK. Připojování cizí techniky do vnitřní sítě ZK je zakázáno. Výjimky povoluje Správce IS.
   6. Na přidělenou techniku ZK nesmí být bez souhlasu Správce IS nahráván, instalován nebo z ní odebírán žádný software.
   7. Při opuštění pracoviště musí druhá smluvní strana provést jeho zajištění (pracovní stanice, nosiče dat, papírové dokumenty) před neoprávněným přístupem.
   8. Druhá smluvní strana je povinna uchovávat přenosná paměťová média na bezpečném místě, např. v uzamčené skříni, stolu nebo místnosti. Originální datová média a záložní kopie citlivých souborů musí být chráněna nejen proti odcizení a zneužití, ale i proti poškození nebo zničení.
   9. Druhá smluvní strana je povinna chránit přidělené pracovní stanice a data na nich uložená proti odcizení, proti neoprávněnému přístupu a proti poškození nebo zničení.
6. **Důvěrnost informací**
   1. Za důvěrné informace ZK (bez ohledu na formu jejich zachycení) se považují zejména veškeré technické informace o IS ZK, které nebyly ze strany ZK označeny jako veřejné.
   2. Druhá smluvní strana je povinna zajistit odpovídající ochranu všech důvěrných informací.
7. **Ochrana dat a informačních aktiv**
   1. Data ZK jsou ve vlastnictví ZK, který k nim má primární užívací právo.
   2. Druhá smluvní strana je povinna chránit všechna data ZK, se kterými přijde do styku. Všechny nové aplikace a aktualizace musí být ověřeny v testovací prostředí. Používat ostrá data pro zkušební a testovací účely je zakázáno. Výjimku může v odůvodněných případech povolit pouze vedoucí odboru ICT.
   3. Druhá smluvní strana odpovídá za všechna převzatá data (elektronická a tištěná), způsob jejich použití a ochranu před neoprávněným přístupem a zneužitím. Není-li ve smlouvě stanoveno jinak, před ukončením smluvního vztahu druhá smluvní strana vrátí všechna převzatá data a všechny jejich kopie bezpečně zlikviduje.
   4. Druhá smluvní strana je do protokolárního předání pracovníkům ZK odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit. Dále je povinna vytvořit a průběžně aktualizovat plán zálohování.
   5. Ukládání pracovních dat je možné pouze na místa, která určí odpovědná osoba.
   6. Druhá smluvní strana nesmí zobrazovat, měnit, mazat nebo kopírovat citlivá data, zejména pak osobní údaje, pokud to nesouvisí se schváleným účelem přístupu.
   7. Vadná zařízení (včetně pevných disků) s nešifrovanými citlivými daty mohou být druhou smluvní stranou předány externím servisním specialistům pouze po schválení Správcem IS nebo vedoucím oddělení serverové a síťové infrastruktury, Odboru informačních a komunikačních technologií.
   8. Pokud druhá smluvní strana při práci v IS ZK přijde do styku s osobními údaji dle platné legislativy nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
   9. Všechna nepotřebná data (elektronická, na mediích i papírová) musí být druhou smluvní stranou vždy neprodleně bezpečně skartována.
   10. Druhá smluvní strana je povinna všechny zásahy na serverech předem odsouhlasit se Správcem IS a zaznamenat stanoveným způsobem.
   11. Druhá smluvní strana je povinna řídit změny v konfiguraci systému, při realizaci aktualizací, zálohování apod. Druhá smluvní strana navrhne předmětné změny, tyto zdokumentuje a předloží Správci IS. Druhá smluvní strana poskytuje součinnost Správci IS při vyhodnocení rizik (např. prostřednictvím analýzy rizik) a potencionálních dopadů změny. Druhá smluvní strana je povinna v případě vyžádání Správcem IS provést testování funkčnosti a bezpečnosti změny. Změnu provede až po odsouhlasení Správcem IS, přičemž vždy takovým způsobem, aby byla zaručena i možnost navrácení do předchozího stavu.
   12. Druhá smluvní strana je povinna řídit rizika a na požádání informovat Správce IS jakým způsobem řídí rizika (včetně popisu způsobu řízení rizik či metody řízení) a jaká jsou zbytková rizika související s předmětem dodávané služby. Správce IS má právo způsob řízení rizik u druhé smluvní strany ověřit a druhá strana je povinna poskytnout Správci IS nezbytnou součinnost.
8. **Ochrana proti škodlivým kódům**
   1. Druhá smluvní strana je povinna všechny servery a pracovní stanice v IS ZK a pracovní stanice druhé smluvní strany, které se připojují k IS ZK, vybavit antivirovým skenerem. Výjimky schvaluje Správce IS.
   2. Pokud některé aplikace nabízejí možnost zvýšené ochrany, musí být odpovídajícím způsobem nastavena. Způsob nastavení schvaluje Správce IS.
   3. Nebezpečné typy souborů jsou blokovány na hranicích bezpečnostního perimetru. Výjimky schvaluje v řádně odůvodněných a zdokumentovaných případech Správce IS.
   4. Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům nejen pro nastavení a využívání prostředků ZK, ale i na přístupových bodech a svých vlastních zařízeních.
   5. Druhá smluvní strana je povinna pro zajištění provozní a komunikační bezpečnosti provádět pravidelné sledování a analýzy technických zranitelností a jejich následné ošetření.
9. **Bezpečnostní incidenty**
   1. Druhá smluvní strana je povinna neprodleně (telefonicky a následně písemně např. prostřednictvím Helpdesku, e-mailu apod.) hlásit odpovědným osobám porušení těchto Bezpečnostních pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty, a to zejména ve vztahu k plnění smlouvy, jejíž přílohou jsou tato bezpečnostní pravidla, zjištěná zranitelná místa, nedostatky a nesoulady. Při jejich prošetřování a odstraňování je povinna poskytnout účinnou součinnost.
   2. Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení Správcem IS.
10. **Používání internetu**
    1. Druhá smluvní strana může používat při práci v IS ZK internet pouze pro účely plnění smlouvy a za podmínky dodržování všech všeobecně uznávaných bezpečnostních pravidel, platných pro práci s internetem. Stahování souborů, používání FTP a jiných služeb je možné jen po dohodě se Správcem IS.
    2. Pokud není ve smlouvě stanoveno jinak, není povoleno využívat elektronickou korespondenci z prostředí ZK.
11. **Tisk**
    1. Druhá smluvní strana může tisknout na tiskárnách ZK pouze s povolením odpovědné osoby. Tisknout je povoleno pouze dokumenty související s předmětem smlouvy a při tisku je nutno šetřit spotřební materiál.
    2. Druhá smluvní strana je povinna zabezpečit tištěné dokumenty proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí, až do jejich bezpečné skartace.
12. **Použití kryptografických technik** 
    1. Kryptografické metody musí být druhou smluvní stranou použity vždy, jestliže není možné bezpečnost dat nebo komunikace zaručit jinými způsoby. Jedná se např. o přenosy citlivých dat prostřednictvím nedůvěryhodných sítí nebo přístup externích subjektů k citlivým zdrojům.
    2. Druhá smluvní strana je oprávněna použít pouze takové kryptografické algoritmy a protokoly a v takovém užití (např. odpovídající délky klíčů), které jsou podle platných standardů všeobecně považovány za bezpečné.
    3. Druhá smluvní strana není oprávněna použít proprietární nebo obecně neuznávané algoritmy, výjimky povoluje Správce IS.
13. **Předání dat**
    1. Data vzniklá při používání systému musí být exportovatelná v otevřeném, strukturovaném a strojově čitelném formátu (např. formát csv, xml, json), přičemž přesný formát odsouhlasuje Správce IS. K exportovaným datům bude dodán popis struktury, význam a vazby mezi jednotlivými daty.
    2. Data musí být předána při ukončení smluvního vztahu a kdykoliv na vyžádání Správce IS. V případě, že Správce IS při ukončení smluvního vztahu rozhodne, že již data nejsou potřebná, zajistí druhá smluvní strana jejich bezpečnou likvidaci. Konkrétní způsob likvidace dat musí být odsouhlasen Správcem IS.
    3. Druhá smluvní strana je povinna poskytnout nezbytnou součinnost (včetně případné migrace dat) týkající se změn v IS ZK, a to kdykoliv na požádání Správce IS nebo v případě ukončení smlouvy, jejíž přílohou jsou tato bezpečnostní pravidla.
14. **Smluvní pokuty**
    1. Pokud druhá smluvní strana poruší bezpečnostní pravidla uvedená v článku 1, písm. b) až d), článku 2, písm. b), c), d), f), g), článku 3, písm. a), článku 4, písm. b) až e), článku 5, písm. e) až j), článku 7, písm. b) až l), článku 8, písm. a), d), e), článku 9, písm. a), b), článku 10, písm. a), článku 11, písm. b), článku 12, písm. a) až c), článku 13, písm. a) až c) je Zlínský kraj oprávněn po druhé smluvní straně požadovat a druhá smluvní strana je povinna v případě uplatnění tohoto práva zaplatit Zlínskému kraji pokutu za každý zjištěný případ porušení. Výše smluvní pokuty je uvedena ve smlouvě.