Smlouva o poskytování služeb Technologického centra Jihočeského kraje

uzavřená ve smyslu ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb.,
občanský zákoník (dále též „občanský zákoník“)

Jihočeský kraj
se sídlem: U Zimního stadionu 1952/2, 370 01 České Budějovice
zastoupený: MUDr. Martinem Kubou, hejtmanem kraje
IČO: 70890650

dále též „poskytovatel“

a

Správa a údržba silnic Jihočeského kraje
se sídlem: Nemanická 2133/10, 370 01 České Budějovice
zastoupená: Ing. Andreou Jankovcovou, ředitelkou
IČO: 70971641

dále též „příjemce“

společně též „smluvní strany“

uzavírají níže uvedeného dne tuto smlouvu o poskytování služeb.

1 Úvodní ustanovení

1.1 Poskytovatel je provozovatelem Technologického centra Jihočeského kraje (TC JčK), v rámci kterého je možné provozovat hostované služby pro další subjekty, a tedy i pro příjemce.

1.2 Příjemce má zájem na vybudování Informačního systému dopravní infrastruktury Jihočeského kraje (ISDIJK), za tímto účelem připravuje podání žádosti o poskytnutí dotace do výzvy č. 9 Integrovaného regionálního operačního programu (IROP 2021 – 2027). Tento systém by běžel (byl hostován) v rámci TC JčK. Předpokladem pro realizaci předmětu této smlouvy je podmínka získání dotace z IROP příjemcem.

1.3 Smluvní strany touto smlouvou upravují svá práva a povinnosti v rámci poskytování služeb TC JčK a deklarují závazek společné vůle hledat optimální variantu pro zajištění hostování ISDIJK v prostředí TC JčK.

2 Práva a povinnosti stran

2.1 Poskytovatel se k naplnění obsahu spolupráce dle této smlouvy zavazuje zejména:

a) spolupracovat s příjemcem při hledání optimální varianty hostování ISDIJK v TC JčK,
b) vyčlenit, připravit a zprovoznit kapacitu TC JčK pro zajištění provozu ISDIJK, zejména v podobě příslušných virtuálních serverů a datových úložišť ve v optimální variantě definované společně poskytovatelem a příjemcem,
c) poskytnout technické kapacity TC JčK pro provoz ISDIJK,
d) zajistit provozní služby TC JčK v rozsahu 24x7 a servisní služby TC JčK v rozsahu 8x5,
e) zajistit požadavky na bezpečnost provozu TC JčK (kybernetická bezpečnost, mlčenlivost a ochrana osobních údajů).

2.2 Příjemce se k naplnění obsahu spolupráce dle této Smlouvy zavazuje zejména:

a) poskytovat poskytovateli řádně a včas nezbytnou součinnost nutnou pro stanovení optimální varianty hostování ISDIJK v TC JčK a pro řádný výkon jeho povinností dle této smlouvy,
b) poskytnout poskytovateli na vyžádání veškeré informace nezbytné pro definování parametrů optimální varianty řešení hostování ISDIJK v TC JčK a pro výkon jeho povinností dle této smlouvy.

Smluvní strany jsou povinny zachovávat mlčenlivost o všech skutečnostech a informacích, které jim byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděly, vyjma těch, které jsou v okamžiku, kdy se s nimi některá ze stran seznámila, prokazatelně veřejně přístupné nebo těch, které se bez zavinění kterékoli ze stran veřejně přístupnými stanou (dále jen „důvěrné informace“). Smluvní strany nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch druhé smluvní strany.

3 Cena a platební podmínky

3.1 Smluvní strany se dohodly, že služby TC JčK budou pro potřeby ISDIJK poskytovány bezplatně.

4 Komunikace mezi stranami

4.1 Ve věcech odborných a technických jsou určeny následující kontaktní osoby.

Na straně poskytovatele:

Ing. Václav Hála, hala@kraj-jihocesky.cz, mobil: [redacted]

p. Jan Suchan, suchan@kraj-jihocesky.cz, mobil: [redacted]

Na straně příjemce:

p. Jan Varecha, varecha@susjk.cz, mobil: [redacted]

5 Ukončení smlouvy

5.1 Tuto smlouvu je možné ukončit dohodou stran.

5.2 Smlouvu je možné ukončit výpovědí. Výpověď musí být písemná, a nemusí být odůvodněná. Výpovědní doba činí 3 měsíce, a počne běžet prvním dnem měsíce následujícího po doručení výpovědi druhé straně.

5.3 Tato smlouva se od počátku ruší tehdy, pokud nedojde k poskytnutí dotace z IROP.

6 Závěrečná ujednání

6.1 Smlouva může být měněna pouze písemnými dodatky.

6.2 Smlouva je uzavírána v elektronické podobě, kdy každá ze stran obdrží její elektronický originál opatřený elektronickými podpisy.

6.3 Příjemce bere na vědomí, že smlouva bude uveřejněna v registru smluv zřízeného podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Příjemce prohlašuje, že tato smlouva neobsahuje údaje, které tvoří předmět jeho obchodního tajemství podle § 504 občanského zákoníku.

6.4 Smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v registru smluv. Zveřejnění zajistí poskytovatel.

6.5 Uzavření této smlouvy bylo schváleno usnesením Rady Jihočeského kraje č. 888/2023/RK-73 ze dne 17. 8. 2023.

6.6 Strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují své podpisy.

6.7 Součástí této smlouvy jsou následující přílohy:

- Příloha č. 1- bezpečnostní pravidla pro dodavatele
- Příloha č. 2- informace o zpracování osobních údajů

V Českých Budějovicích dne

Elektronický podpis - 21.8.2023
Certifikát autora podpisu :
Jméno : MUDr. Martin Kuba
Vydal : PostSignum Qualified CA 4
Platnost do : 20.12.2023 12:17:21+00:00 +01:00

Za poskytovatele

MUDr. Martin Kuba, hejtman kraje

V Českých Budějovicích dne

Ing. Andrea Jankovcová
Digitálně podepsal Ing. Andrea Jankovcová
Datum: 2023.08.21 14:07:14 +02'00'

Za příjemce

Ing. Andrea Jankovcová, ředitelka

Příloha č. 1- bezpečnostní pravidla pro dodavatele

Pro účely této přílohy se pojmem „dodavatel“ myslí „příjemce“, a případné další osoby, které buď pro poskytovatele nebo pro příjemce vykonávají požadované služby.

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva KÚ JK, ke kterým mají přístup Dodavatelé.

A.1 Základní odpovědnosti Dodavatele

Dodavatel řešení:

a) Je povinen dodržovat požadavky na bezpečnost informací v souladu s platnými zákony ČR.
b) Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KÚ JK, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.
c) Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
d) Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s úřadem.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarem IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

A.2 Ochrana Aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím KÚ JK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KÚ JK (prioritně ve smlouvě, prohlášením Dodavatele, formulářem, …) 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).

A.3 Přístup k ICT/IS

Přihlášení Dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

A.4 Ochrana před škodlivým softwarem

Dodavatel je povinen:

a) 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 č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a zejména vyhláškou č. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.
b) 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.
c) Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.
d) Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

A.5 Řízení bezpečnostních rizik

Dodavatel je povinen zajistit, že:

a) Hesla pracovníků Dodavatele nebudou zaznamenávána v otevřené podobě.
b) Vzájemnou spolupráci a komunikaci mezi Dodavatelem a KÚ JK při řešení ICT bezpečnostní rizik

A.6 Hlášení

Dodavatel je povinen KÚ JK hlásit:

a) nestandardní situace při práci v ICT/IS;
b) bezpečnostní události nad ICT/IS;

c) bezpečnostní slabiny v ICT/IS Poskytovatele.

A.7 Kontrola a audit Dodavatele

KÚ JK má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostních pravidel Objednatele či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele, a to minimálně 1x za 12 měsíců.

A.8 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, který má právo výjimku udělit.

Schváleno: Bezpečnostní komise – Výbor pro řízení kybernetické bezpečnosti

Příloha č. 2- Ochrana a zpracování osobních údajů

Pro účely této přílohy se pojmy „objednatel“ a „zhotovitel“ budou vždy vykládat dle konkrétní situace příjemce a poskytovatele. Většinou bude poskytovatel v pozici objednatele, a tedy i správce osobních údajů, nicméně může nastat i opačná situace.

1. Objednatel a zhotovitel 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. Zhotovitel bere na vědomí, že se ve smyslu všech výše uvedených právních předpisů 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, se všemi pro něj vyplývajícími důsledky a povinnostmi.
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 opatření k zabezpečení ochrany osobních údajů a základních práv a svobod subjektů údajů při zpracování osobních údajů zpracovatelem.
4. Zpracovatel se zavazuje zpracovávat pouze a výlučně ty osobní údaje, které jsou nutné k výkonu jeho činnosti dle této smlouvy.
5. Zpracovatel je oprávněn zpracovávat osobní údaje dle této smlouvy pouze a výlučně po dobu účinnosti této smlouvy, stanovené v čl. 10 smlouvy „Závěrečná ustanovení“.
6. Zpracovatel je oprávněn zpracovávat osobní údaje pouze za účelem stanoveném v předmětu Servisní smlouvy.
7. Zpracovatel je povinen se při zpracování osobních údajů řídit výslovnými pokyny správce, budou-li mu takové uděleny, ať již ústní či písemnou formou. Za písemnou formu se považuje i elektronická komunikace, včetně emailu. Zpracovatel je povinen neprodleně správce informovat, pokud dle jeho názoru udělený pokyn správce porušuje Nařízení nebo jiné předpisy na ochranu osobních údajů.
8. Zpracovatel je povinen zajistit, že osoby, jimiž bude provádět plnění dle této smlouvy, se zavážou k mlčenlivosti ohledně veškeré činnosti související s touto smlouvou, zejm. pak k mlčenlivosti ve vztahu ke všem osobním údajům, ke kterým budou mít přístup, nebo s kterými přijdou do kontaktu.
9. Zpracovatel je povinen, ve smyslu čl. 32 Nařízení přijmout, s ohledem na stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, zejm. pak osobní údaje zabezpečit vůči náhodnému či nezákonnému zničení, ztrátě, změně, zpřístupnění neoprávněným stranám, zneužití či jinému způsobu zpracování v rozporu s Nařízením.
10. Zpracovatel je povinen písemně seznámit správce s jakýmkoliv podezřením na porušení nebo skutečným porušením bezpečnosti zpracování osobních údajů podle ustanovení této smlouvy, např. jakoukoliv odchylkou od udělených pokynů, odchylkou od sjednaného přístupu pro správce, plánovaným zveřejněním, upgradem, testy apod., kterými může dojít k úpravě nebo změně zabezpečení nebo zpracování osobních údajů, jakýmkoliv podezřením z porušení důvěrnosti, jakýmkoliv podezřením z náhodného či nezákonného zničení, ztráty, změny, zpřístupnění neoprávněným stranám, zneužití či jiného způsobu zpracování osobních údajů v rozporu s Nařízením. Správce bude neprodleně seznámen s jakýmkoliv podstatným porušením těchto ustanovení o zpracování dat.
11. Zpracovatel není oprávněn, ve smyslu čl. 28 Nařízení, zapojit do zpracování osobních údajů dalšího zpracovatele (zákaz řetězení zpracovatelů), bez předchozího schválení a písemného souhlasu správce.
12. Zpracovatel je povinen a zavazuje se k veškeré součinnosti se správcem, o kterou bude požádán v souvislosti se zpracováním osobních údajů nebo která mu přímo vyplývá z Nařízení. Zpracovatel je povinen na vyžádání zpřístupnit správci svá písemná technická a organizační bezpečnostní opatření a umožnit mu případnou kontrolu, audit či inspekci dodržování předložených technických a organizačních bezpečnostních opatření.
13. Po skončení účinnosti této smlouvy nebo v případě předčasného ukončení, je zpracovatel povinen všechny osobní údaje, které má v držení vymazat, a pokud je dosud nepředal správci, předat je správci a dále vymazat všechny existující kopie. Povinnost uvedená v tomto článku neplatí, stanoví-li právní předpis EU, případně vnitrostátní právní předpis zpracovateli osobní údaje ukládat i po skončení účinnosti této smlouvy.