

SMLOUVA O SPOLUPRÁCI

PŘI VZÁJEMNÉM POSKYTOVÁNÍ DAT A DATOVÝCH VÝSTUPŮ GIS

Číslo smlouvy PVS: 0319/22

Číslo smlouvy PVK: SD230506

Číslo smlouvy za TSK: 9/23/3267/015

SMLUVNÍ STRANY

Technická správa komunikací hl. m. Prahy, a.s.

sídlo: Veletržní 1623/24, 170 00 Praha 7 - Holešovice

IČO: 03447286

DIČ: CZ03447286

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 20059

bankovní spojení: PPF banka a.s.

číslo účtu: 2023100003/6000

datová schránka: mivq4t3

zastoupení: Při podpisu Smlouvy a veškerých jejích dodatků jsou oprávněni zastupovat společnost dva členové představenstva společně, z nichž nejméně jeden musí být předsedou anebo místopředsedou představenstva.

(dále jen „**TSK**“ nebo „Objednatel“)

a

Pražská vodohospodářská společnost a.s.

se sídlem: Evropská 866/67, Vokovice, 160 00 Praha 6

IČO: 25656112

DIČ: CZ25656112

zastoupena: Mgr. Martinem Velíkem, na základě plné moci ze dne 1.2.2019

zapsána v obchodním rejstříku vedeném: Městským soudem v Praze pod sp. značkou: B 5290

bankovní spojení:

Česká spořitelna a.s., číslo účtu: 6060522/0800

Československá obchodní banka, a.s., číslo účtu: 117411663/0300

datová schránka: a75fsn2

(dále jen „**PVS**“ nebo „Dodavatel“)

a

Pražské vodovody a kanalizace, a.s.

se sídlem: Ke Kablu 971/1, Hostivař, 102 00 Praha 10

IČO: 25656635

DIČ: CZ25656635

zastoupena: Ing. Petrem Mrkosem, místopředsedou představenstva

Ing. Miluší Polákovou, členkou představenstva

zapsána v obchodním rejstříku vedeném: Městským soudem v Praze pod sp. značkou: B 5297

bankovní spojení: Komerční banka, a.s., číslo účtu: 4000505-031/0100

datová schránka: ec9fspf

(dále jen „**PVK**“ nebo „Dodavatel“)

(TSK, PVS nebo PVK dále společně také jako „**smluvní strany**“ či jednotlivě jako „**strana**“)

Článek 1. Úvodní ustanovení

- 1.1 TSK je společnost založená HMP za účelem správy veřejných komunikací a dalšího souvisejícího majetku ve vlastnictví hlavního města Prahy, jejich oprav a obnovy, údržby městské zeleně. V rámci své běžné činnosti využívá aplikaci GIS (geografický informační systém) pro geografické zobrazování dat o spravovaném majetku hlavního města Prahy, o provádění a plánování staveb apod.
- 1.2 PVS je společnost založená HMP za účelem správy vodovodů a kanalizací pro veřejnou potřebu ve vlastnictví hlavního města Prahy, provozovatelem těchto vodovodů a kanalizací pro veřejnou potřebu je PVK. Obě společnosti společně pro svou běžnou činnost využívají společnou geodatabázi GIS (geografický informační systém) pro geografické zobrazování dat o spravovaném a provozovaném vodohospodářském majetku hlavního města Prahy, o provádění a plánování staveb apod. PVS a PVK se dohodly, že veškeré povinnosti z této smlouvy ve směru k TSK bude zabezpečovat PVK.
- 1.3 Smluvní strany prohlašují, že pro správu a rozvoj aplikací GIS využívá jak TSK na straně jedné, tak PVS a PVK na straně druhé, vlastní technické řešení. Ze strany vlastníka majetku, hlavního města Prahy, není vytvořena žádná aplikace či jiná platforma pro sdílení dat GIS o majetku hlavního města Prahy. Z toho důvodu smluvní strany uzavírají tuto smlouvu s tím, že získané zkušenosti budou předány hlavnímu městu Praze k využití pro sdílení dat GIS mezi odbory a organizacemi zřízenými či společnostmi založenými hlavním městem Prahou.

Článek 2. Předmět smlouvy

- 2.1 Předmětem této smlouvy je vzájemná výměna dat o majetku hlavního města Prahy mezi TSK na straně jedné a PVS a PVK na straně druhé a jejich zobrazování v systému GIS (geografický informační systém) užívaném smluvními stranami, zejména se bude jednat o informace o spravovaném majetku, jeho obnově a stavu. Popis předávaných dat je uveden v příloze č. 4.
- 2.2 Konkrétní specifikace dat a datových výstupů včetně úložiště dat a termínů aktualizace dat budou sjednány zápisem odsouhlaseným zástupci smluvních stran, které určí smluvní strany.

Článek 3. Úhrada nákladů

- 3.1 Smluvní strany prohlašují, že i s ohledem na skutečnost, že předmětem výměny dat budou údaje o majetku hlavního města Prahy, který mají smluvní strany ve správě či provozování, považují smluvní strany vzájemná plnění za vzájemně odpovídající.
- 3.2 Pro zajištění plnění podle této smlouvy smluvní strany nepředpokládají vynaložení dodatečných nákladů nad rámec svého vlastního počítačového vybavení.
- 3.3 Pro daňové účely smluvní strany oceňují hodnotu vzájemně poskytnutých plnění na částku 10 000,- Kč bez DPH ročně. TSK a PVK jsou oprávněni vystavit fakturu na částku 10 000,- Kč bez DPH v průběhu čtvrtého čtvrtletí kalendářního roku účinnosti této smlouvy. Smluvní strany sjednávají možnost vzájemného zápočtu obou faktur.

Článek 4. Další ujednání

- 4.1 Veškerá vzájemně poskytnutá data jsou určena pro interní potřeby smluvních stran a jiným osobám nemohou být předávána. Za interní potřebu smluvní strany se považuje i jednorázové poskytnutí dat v nezbytně nutném rozsahu smluvnímu dodavateli za účelem provedení prací.
- 4.2 Nezbytné bezpečnostní požadavky a opatření z hlediska kybernetické bezpečnosti podrobně upravuje Příloha č. 2, která je nedílnou součástí této smlouvy. Při porušení povinností v oblasti bezpečnostních požadavků a opatření z hlediska kybernetické bezpečnosti ze strany Dodavatele či jeho poddodavatelů, je Dodavatel povinen zaplatit TSK smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý případ porušení sjednané povinnosti.

- 4.3 Další nezbytné bezpečnostní požadavky a opatření z hlediska kybernetické bezpečnosti podrobně upravuje Příloha č. 3, která je nedílnou součástí této smlouvy. Při porušení povinností v oblasti bezpečnostních požadavků a opatření z hlediska kybernetické bezpečnosti ze strany Objednatele či jeho poddodavatelů, je Objednatel povinen zaplatit PVK smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý případ porušení sjednané povinnosti.

Článek 5. Registr smluv

- 5.1 Smluvní strany berou na vědomí, že tato smlouva (text smlouvy bez příloh) podléhá povinnosti uveřejnění prostřednictvím registru smluv dle zákona č. 340/2015 Sb., zákon o registru smluv. Uveřejnění smlouvy v registru smluv zajistí PVS.
- 5.2 Uveřejněním prostřednictvím registru smluv se rozumí vložení elektronického obrazu textového obsahu smlouvy v otevřeném a strojově čitelném formátu a rovněž metadat do registru smluv. Uveřejnění podléhá tato metadata: identifikace smluvních stran, vymezení předmětu smlouvy, cena (případně hodnota předmětu smlouvy, lze-li ji určit), datum uzavření smlouvy.
- 5.3 Smluvní strany výslovně prohlašují, že informace obsažené v části smlouvy určené k uveřejnění v registru smluv včetně metadat neobsahují informace, které nelze poskytnout podle předpisů upravujících svobodný přístup k informacím, a nejsou smluvními stranami označeny za obchodní tajemství.

Článek 6. Souhrnná doložka uzavřená na základě Compliance programu TSK

- 6.1 PVS a PVK berou výslovně na vědomí Etický kodex pro dodavatele/obchodní partnery TSK, a zavazují se jej při plnění této Smlouvy dodržovat, nebo zajistit dodržování odpovídajících povinností ve stejném rozsahu na základě vlastního (jiného) etického kodexu. To se týká jak oblasti obecných Compliance zásad, tak i specifických požadavků vztahujících se k nulové toleranci korupčního jednání a celkovému dodržování zásad slušnosti, poctivosti a dobrých mravů.
- 6.2 PVS a PVK berou dále výslovně na vědomí, že Souhrnná smluvní doložka obsahuje i jiné povinnosti nad rámec odst. 1 výše, a to zejména z oblasti absence mezinárodních a národních sankcí, nebo zamezování střetu zájmů ve smyslu zákona č. 159/2006 Sb. PVS a PVK se zavazují tyto povinnosti dodržovat.
- 6.3 PVS a PVK výslovně prohlašují, že si jsou vědomi kontrolních i sankčních oprávnění TSK vyplývajících ze všech částí Souhrnné smluvní doložky, a že s nimi souhlasí; a v případě, že proti nim budou uplatněny, se zavazují je akceptovat.
- 6.4 Podrobně jsou práva a povinnosti Smluvních stran rozvedeny v příloze č. 1 Souhrnná smluvní doložka, která tvoří nedílnou součást Smlouvy.

Článek 7. Ustanovení společná a závěrečná

- 7.1 Smluvní strany se zavazují dodržovat všechny povinnosti uvedené v této smlouvě.
- 7.2 Změny této smlouvy, zejména změny týkající se předmětu této smlouvy nebo podmínek v této smlouvě upravených, jsou možné pouze formou písemného a číslovaného dodatku na základě dohody smluvních stran. Komunikace mezi smluvními stranami, není-li ve smlouvě stanoveno jinak, postačuje ve formě emailové komunikace.
- 7.3 Smlouva se uzavírá na dobu neurčitou.
- 7.4 Tuto smlouvu je možné ukončit dohodou smluvních stran nebo výpovědí bez udání důvodu. Výpovědní doba činí 6 (šest) měsíců počínaje prvním kalendářním dnem měsíce následujícího po měsíci, ve kterém dojde k doručení písemné výpovědi druhé, eventuálně druhé a třetí smluvní straně. Tato výpovědní doba skončí nejpozději uplynutím doby trvání této smlouvy.
- 7.5 Od této smlouvy lze odstoupit v případech stanovených obecně závaznými právními předpisy.

- 7.6 Smluvní strany shodně prohlašují, že tato smlouva nabývá platnosti dnem podpisu všemi smluvními stranami a účinnosti dnem uveřejnění v registru smluv dle zákona o registru smluv.
- 7.7 Smluvní strany dále shodně prohlašují, že tato smlouva odpovídá jejich svobodné a vážné vůli, což stvrzují všechny smluvní strany podpisy svých oprávněných zástupců níže na této smlouvě uvedenými.
- 7.8 Smluvní strany dále prohlašují, že tato smlouva je vyhotovena v 4 (čtyřech) stejnopisech, kdy PVS a PVK obdrží po 1 (jednom) stejnopisu a TSK po 2 (dvou) stejnopisech. V případě, že je smlouva uzavírána elektronicky za využití uznávaných elektronických podpisů, postačí jedno vyhotovení smlouvy, na kterém jsou zaznamenány uznávané elektronické podpisy zástupců všech smluvních stran.
- 7.9 Nedílnou součástí této Smlouvy jsou přílohy:
- Příloha č. 1 – Souhrnná doložka do smluv uzavíraných Technickou správou komunikací hl. m. Prahy, a.s.
 - Příloha č. 2 – Bezpečnostní požadavky a opatření
 - Příloha č. 3 – Bezpečnostní požadavky a opatření
 - Příloha č. 4 – Popis předávaných dat

V Praze dne: dle data el. podpisu

V Praze dne: dle data el. podpisu

TSK
Mgr. Jozef Sinčák, MBA
Předseda představenstva

PVK
Ing. Petr Mrkos
Místopředseda představenstva

TSK
PhDr. Filip Hájek,
Místopředseda představenstva

PVK
Ing. Miluše Poláková,
Člen představenstva

V Praze dne: dle data el. podpisu

PVS
Ing. Pavel Válek, MBA
Předseda představenstva

PVS
Mgr. Martin Velík
Místopředseda představenstva

Příloha č. 1 – Souhrnná doložka do smluv uzavíraných Technickou správou komunikací hl. m. Prahy, a.s.

Příloha č. 2 - Bezpečnostní požadavky a opatření TSK

1. Objednatel byl v srpnu 2021 Národním úřadem pro kybernetickou bezpečnost (dále jen „NÚKIB“) určen jako provozovatel základní služby dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“), ve znění pozdějších předpisů. Objednatel, jakožto povinná osoba dle ZoKB je povinen realizovat celou řadu bezpečnostních opatření, řídit se příslušnou legislativou a provádět činnosti dle nařízení vydávaných NÚKIB. V průběhu plnění smlouvy tak může dojít k situaci, kdy Objednatel bude povinen realizovat bezpečnostní opatření, která mohou mít dopad na odebírané služby, provozované informační systémy a technická zařízení (např. na jejich rozsah, kvalitu, bezpečnost, používané technologie apod.). Pro případ, že takováto situace nastane, zavazují se obě smluvní strany vstoupit v jednání s cílem dosáhnout vzájemné dohody. Pokud by nebylo možné dohody dosáhnout, je Objednatel oprávněn smlouvu ukončit, a to ve lhůtě 1 měsíce od doručení oznámení o ukončení smlouvy Dodavateli z výše uvedených důvodů.
2. Dodavatel je povinen poskytovat Objednateli součinnost při plnění povinností Objednatele podle ZoKB včetně preventivních aktivit a součinnost při plnění povinností Objednatele vyplývajících z rozhodnutí státních orgánů vykonávajících působnost na úseku kybernetické bezpečnosti. Dodavatel je při poskytování předmětu plnění dle této Smlouvy dále povinen dodržovat veškerá bezpečnostní opatření vyplývající ze ZoKB.
3. Objednatel považuje Dodavatele za významného dodavatele v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
4. Dodavatel se zavazuje přijímat, neustále kontrolovat a zvyšovat bezpečnostní opatření nezbytná k zajištění ochrany informací, zejména proti neoprávněnému nebo nahodilému přístupu, neoprávněným přenosům (důvěrnost informací), změnám či podvržení (integrita informací) a zničením nebo ztrátám (dostupnost informací).
5. Dodavatel se zavazuje prokázat, že zavedl a po celou dobu trvání smlouvy udržuje bezpečnostní opatření dle ujednání v této Smlouvě, a to bez zbytečného odkladu po vyžádání ze strany Objednatele. Objednatel má právo nejen v případě bezpečnostního incidentu, provést u Dodavatele kontrolu a audit bezpečnostních opatření souvisejících s plněním Smlouvy. O této kontrole, jejím rozsahu, kontrolujících osobách, bude Objednatel informovat Dodavatele minimálně s předstihem deseti (10) pracovních dnů a Dodavatel nemá právo tuto kontrolu odmítnout.
6. V případě, kdy Dodavatel pro plnění předmětu Smlouvy využívá poddodavatele, je Dodavatel povinen zajistit promítnutí bezpečnostních požadavků uvedených ve Smlouvě i na tyto poddodavatele.
7. Dodavatel se zavazuje při poskytování plnění pro Objednatele dodržovat příslušná ustanovení bezpečnostních politik (včetně relevantních metodik a postupů) předaných Dodavateli Objednatelem, pokud byl Dodavatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Dodavateli, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu Dodavateli na sdílené úložiště aj.)
8. V případě změn předmětu plnění Smlouvy, procesů, prostředků nebo technologií souvisejících s plněním Smlouvy na straně Dodavatele či jeho partnerů, které mají či mohou mít vliv na bezpečnost informací, je Dodavatel povinen přezkoumávat jejich možné dopady, určovat významné změny a oznamovat je Objednateli. V případě významných změn je povinností Dodavatele zdokumentovat jejich řízení a provést analýzu rizik: Na základě výsledků analýzy rizik Dodavatel přijme opatření za účelem snížení nepříznivých dopadů a aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci. V případě informačních a komunikačních systémů Dodavatel dále zajistí testování změn a jejich dopadů na bezpečnost informací a v případě zjištění, že došlo ke snížení ochrany informací přijme další

odpovídající bezpečnostní opatření, případně navrátí informační a komunikační systém do původního stavu.

9. Dodavatel je povinen informovat Objednatele o:

- jakémkoliv bezpečnostním incidentu, který vznikne v jeho informačním systému (včetně přístupu neoprávněné třetí strany, ztráty dat, poškození integrity dat, zavlečení malwaru a/nebo nestandardního použití informačních systémů používaných pro plnění Smlouvy), a to vždy, kdy takový incident i potenciálně může ovlivnit informační systém, služby, informace nebo data Objednatele
- Způsobu řízení rizik na straně Dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy
- Významné změně ovládnutí Dodavatele podle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále „zákon o obchodních korporacích“), nebo změně vlastnictví zásadních aktiv

10. Dodavatel je povinen předat Objednateli data a informace o informačních a komunikačních systémech, aktivech Objednatele i data a informace z informačních a komunikačních systémů Objednatele, které má k dispozici v souvislosti s plněním předmětu této Smlouvy, do pěti (5) pracovních dní od ukončení platnosti této Smlouvy. Dodavatel dále zruší do tří (3) pracovních dní od ukončení platnosti této Smlouvy, veškeré vzdálené přístupy k informačním systémům Objednatele, které vznikly na základě plnění Smlouvy.

11. Dodavatel při předání Díla/Poskytnutí služby předloží Objednateli v rámci předání dat, informací a provozních údajů návrhy pro řízení kontinuity činností a havarijní plány v rozsahu plnění předmětu Smlouvy. Tyto dokumenty budou obsahovat způsoby, jakými lze zajistit obnovu funkcionality po havárii či kybernetickém útoku a příp. popis řešení s omezenou funkcionalitou po období obnovy do plné funkcionality. Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace. Dodavatel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli dokumentaci v následujícím rozsahu:

- strategie obnovy
- dokumentace skutečného provedení
- popis autorizačního konceptu a oprávnění
- zálohovací a archivační postupy
- instalační a konfigurační postupy
- bezpečnostní nastavení

12. Dodavatel zajistí, aby předávaná data, informace a provozní údaje byly pro Objednatele v čitelném formátu, systematizované a v případě ukončení Smlouvy použitelné pro přenos do jiných systémů. Za čitelný formát jsou pro účely předávání dat považovány formáty CSV, HTML/XHTML JPEG, PDF, RDF, RTF TXT a XML

13. V termínu do deseti (10) pracovních dní od ukončení platnosti této Smlouvy je Dodavatel povinen zničit bezpečným způsobem všechna nepotřebná data a informace vzniklé při plnění Smlouvy, které má k dispozici v elektronické nebo listinné formě, vypracovat protokol o zničení těchto dat a informací a tento protokol předat do patnácti (15) pracovních dní Objednateli. Povinnost bezpečně zničit data a informace se vztahuje i na jejich případné kopie. Dále je Dodavatel povinen bezpečně zničit i data, která vznikla na straně Dodavatele, či jeho smluvních partnerů, v průběhu plnění Smlouvy (např. logy událostí, monitoring provozu apod.), a to vyjma těch dat a informací, které je na základě jiné právní povinnosti povinen po určitou dobu uchovávat. Takováto data a informace Dodavatel bezpečným způsobem zničí v okamžiku, kdy jejich uchování již nebude nezbytné.

14. V případě, kdy dojde ke změně kontroly nad Dodavatelem dle zákona o obchodních korporacích, či ekvivalentního postavení, nebo změně kontroly nad zásadními aktivy využívanými Dodavatelem

k plnění podle smlouvy, má Objednatel právo odstoupit od Smlouvy s okamžitými účinky ke dni doručení odstoupení od smlouvy Dodavateli.

V případě této přílohy č. 2 vystupuje TSK jako Objednatel.

Příloha č. 3 - Bezpečnostní požadavky a opatření PVK a PVS

1. Dodavatel byl v září 2021 Národním úřadem pro kybernetickou bezpečnost (dále jen „NÚKIB“) určen jako provozovatel základní služby dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“), ve znění pozdějších předpisů. Dodavatel, jakožto povinná osoba dle ZoKB je povinen realizovat celou řadu bezpečnostních opatření, řídit se příslušnou legislativou a provádět činnosti dle nařízení vydávaných NÚKIB. V průběhu plnění smlouvy tak může dojít k situaci, kdy Dodavatel bude povinen realizovat bezpečnostní opatření, která mohou mít dopad na odebírané služby, provozované informační systémy a technická zařízení (např. na jejich rozsah, kvalitu, bezpečnost, používané technologie apod.). Pro případ, že takováto situace nastane, zavazují se obě smluvní strany vstoupit v jednání s cílem dosáhnout vzájemné dohody. Pokud by nebylo možné dohody dosáhnout, je Dodavatel oprávněn smlouvu ukončit, a to ve lhůtě 1 měsíce od doručení oznámení o ukončení smlouvy Objednateli z výše uvedených důvodů.
2. Objednatel je povinen poskytovat Dodavateli součinnost při plnění povinností Dodavatele podle ZoKB včetně preventivních aktivit a součinnost při plnění povinností Dodavatele vyplývajících z rozhodnutí státních orgánů vykonávajících působnost na úseku kybernetické bezpečnosti. Objednatel je při poskytování předmětu plnění dle této Smlouvy dále povinen dodržovat veškerá bezpečnostní opatření vyplývající ze ZoKB.
3. Dodavatel považuje Objednatele za významného dodavatele v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
4. Objednatel se zavazuje přijímat, neustále kontrolovat a zvyšovat bezpečnostní opatření nezbytná k zajištění ochrany informací, zejména proti neoprávněnému nebo nahodilému přístupu, neoprávněným přenosům (důvěrnost informací), změnám či podvržení (integrita informací) a zničením nebo ztrátám (dostupnost informací).
5. Objednatel se zavazuje prokázat, že zavedl a po celou dobu trvání smlouvy udržuje bezpečnostní opatření dle ujednání v této Smlouvě, a to bez zbytečného odkladu po vyžádání ze strany Dodavatele. Dodavatel má právo nejen v případě bezpečnostního incidentu, provést u Objednatele kontrolu a audit bezpečnostních opatření souvisejících s plněním Smlouvy. O této kontrole, jejím rozsahu, kontrolujících osobách, bude Dodavatel informovat Objednatele minimálně s předstihem deseti (10) pracovních dnů a Objednatel nemá právo tuto kontrolu odmítnout.
6. V případě, kdy Objednatel pro plnění předmětu Smlouvy využívá poddodavatele, je Objednatel povinen zajistit promítnutí bezpečnostních požadavků uvedených ve Smlouvě i na tyto poddodavatele.
7. Objednatel se zavazuje při poskytování plnění pro Dodavatele dodržovat příslušná ustanovení bezpečnostních politik (včetně relevantních metodik a postupů) předaných Objednateli dodavatelem, pokud byl Objednatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Dodavatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Objednateli, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu Objednateli na sdílené úložiště aj.)
8. V případě změn předmětu plnění Smlouvy, procesů, prostředků nebo technologií souvisejících s plněním Smlouvy na straně Objednatele či jeho partnerů, které mají či mohou mít vliv na bezpečnost informací, je Objednatel povinen přezkoumávat jejich možné dopady, určovat významné změny a oznamovat je dodavateli. V případě významných změn je povinností Objednatele zdokumentovat jejich řízení a provést analýzu rizik: Na základě výsledků analýzy rizik Objednatel přijme opatření za účelem snížení nepříznivých dopadů a aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci. V případě informačních a komunikačních systémů Objednatel dále zajistí testování změn a jejich dopadů na bezpečnost informací a v případě zjištění, že došlo ke snížení ochrany informací přijme další

odpovídající bezpečnostní opatření, případně navrátí informační a komunikační systém do původního stavu.

9. Objednatel je povinen informovat Dodavatele o:
 - jakémkoliv bezpečnostním incidentu, který vznikne v jeho informačním systému (včetně přístupu neoprávněné třetí strany, ztráty dat, poškození integrity dat, zavlečení malwaru a/nebo nestandardního použití informačních systémů používaných pro plnění Smlouvy), a to vždy, kdy takový incident i potenciálně může ovlivnit informační systém, služby, informace nebo data Dodavatele
 - Způsobu řízení rizik na straně Objednatele a o zbytkových rizicích souvisejících s plněním Smlouvy
 - Významné změně ovládnutí Objednatele podle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále „zákon o obchodních korporacích“), nebo změně vlastnictví zásadních aktiv
10. Objednatel je povinen předat dodavateli data a informace o informačních a komunikačních systémech, aktivech dodavatele i data a informace z informačních a komunikačních systémů Dodavatele, které má k dispozici v souvislosti s plněním předmětu této Smlouvy, do pěti (5) pracovních dní od ukončení platnosti této Smlouvy. Objednatel dále zruší do tří (3) pracovních dní od ukončení platnosti této Smlouvy, veškeré vzdálené přístupy k informačním systémům Dodavatele, které vznikly na základě plnění Smlouvy.
11. Objednatel při předání Díla/Poskytnutí služby předloží Dodavateli v rámci předání dat, informací a provozních údajů návrhy pro řízení kontinuity činností a havarijní plány v rozsahu plnění předmětu Smlouvy. Tyto dokumenty budou obsahovat způsoby, jakými lze zajistit obnovu funkcionality po havárii či kybernetickém útoku a příp. popis řešení s omezenou funkcionalitou po období obnovy do plné funkcionality. Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace. Objednatel se v rámci poskytovaného plnění pro Dodavatele zavazuje předat Dodavateli dokumentaci v následujícím rozsahu:
 - strategie obnovy
 - dokumentace skutečného provedení
 - popis autorizačního konceptu a oprávnění
 - zálohovací a archivační postupy
 - instalační a konfigurační postupy
 - bezpečnostní nastavení
12. Objednatel zajistí, aby předávaná data, informace a provozní údaje byly pro Dodavatele v čitelném formátu, systematizované a v případě ukončení Smlouvy použitelné pro přenos do jiných systémů. Za čitelný formát jsou pro účely předávání dat považovány formáty CSV, HTML/XHTML JPEG, PDF, RDF, RTF TXT a XML
13. V termínu do deseti (10) pracovních dní od ukončení platnosti této Smlouvy je Objednatel povinen zničit bezpečným způsobem všechna nepotřebná data a informace vzniklé při plnění Smlouvy, které má k dispozici v elektronické nebo listinné formě, vypracovat protokol o zničení těchto dat a informací a tento protokol předat do patnácti (15) pracovních dní Dodavateli. Povinnost bezpečně zničit data a informace se vztahuje i na jejich případné kopie. Dále je Objednatel povinen bezpečně zničit i data, která vznikla na straně Objednatele, či jeho smluvních partnerů, v průběhu plnění Smlouvy (např. logy událostí, monitoring provozu apod.), a to vyjma těch dat a informací, které je na základě jiné právní povinnosti povinen po určitou dobu uchovávat. Takováto data a informace Objednatel bezpečným způsobem zničí v okamžiku, kdy jejich uchování již nebude nezbytné.
14. V případě, kdy dojde ke změně kontroly nad Objednatelem dle zákona o obchodních korporacích, či ekvivalentního postavení, nebo změně kontroly nad zásadními aktivy využívanými Objednatelem k plnění podle smlouvy, má Dodavatel právo odstoupit od Smlouvy s okamžitými účinky ke dni doručení odstoupení od smlouvy Objednateli.

V případě této přílohy č. 3 vystupuje PVK jako Objednatel.

Popis předávaných dat ze strany PVS a PVK

1) Data:	Informace o vodovodní a kanalizační infrastruktuře
Forma rozhraní pro předávání dat:	WMS
Doporučená frekvence předávání dat:	Denní
Popis předávaných dat:	Služba s denní aktualizací bude obsahovat zakres kanalizační, vodovodní sítě a objektů s různou třídou přesnosti zaměření, včetně popisných informací, jako je: <ul style="list-style-type: none"> ○ Profil, materiálu ○ Druh vody, typu úseků a objektů ○ Výškové uložení – pokud je známé ○ Míra přesnosti zaměření





























2) Data:	Roční a střednědobý plán obnovy vodohospodářské infrastruktury
Forma rozhraní pro předávání dat:	*.dgn a popisná data ve vhodném formátu
Doporučená frekvence předávání dat:	Roční
Popis předávaných dat:	Data předávané s roční aktualizací, a to vždy po schválení plánu HMP. Data budou obsahovat zakresy rozsahu obnovy liniových úseků a bodový zakres obnovy objektů, včetně popisných informací, jako je: <ul style="list-style-type: none"> ○ Název návrhu investičního záměru NZI ○ Typ stavby a druh vody ○ Návrhy termínu realizace od do ○ Technický popis obnovy

3) Data:	Mapová aplikace „Střednědobý a roční plán obnovy, rekonstrukce, modernizace a rozvoje vodohospodářského majetku pro daný rok“
Forma rozhraní pro předávání dat:	Přístup do mapové aplikace – další možné formy předávaných dat na základě využitelnosti
Doporučená frekvence předávání dat:	Denní
Popis předávaných dat:	Přístup k mapové aplikaci s denní aktualizací popisných dat s roční aktualizací rozsahu investic, a to vždy po schválení plánu HMP. Data v mapové aplikaci jsou členěny dle projektové, povolovací a realizační fáze.

Popis předávaných dat ze strany TSK

1) Data:	Plánované rozsahy investic komunikací ve správě TSK
Forma rozhraní pro předávání dat:	Formu rozhraní dat, doporučenou frekvenci, rozsah a popis předávaných dat určí TSK po provedení analýzy interních datových zdrojů
Doporučená frekvence předávání dat:	
Popis předávaných dat:	

2) Data:	Uzavírka komunikací z důvodu záruční lhůty kom. tělesa
Forma rozhraní pro předávání dat:	WMS
Frekvence aktualizace dat:	Měsíčně
Popis předávaných dat:	Data budou obsahovat zakres rozsahu, včetně popisných informací, jako je: <ul style="list-style-type: none"> ○ Ochranná lhůta začátek ○ Ochranná lhůta konec

3) Data:	Kanalizační infrastruktura
Forma rozhraní pro předávání dat:	WMS
Frekvence aktualizace dat:	Kvartálně
Popis předávaných dat:	<p>Přístup k nadefinovaným grafickým vrstvám :</p> <ul style="list-style-type: none">   201 Uliční vpust'   202 Revizní vstup přípojky   203 Spadiště   204 Odtokové potrubí   205 Drenáže   206 Odvodnění liniové   207 Odvodnění plošné   208 Odvodnění bodové   211 Stoka   212 Vstupní šachta stoky   213 Lapol   221 Nádrže   222 Vstup do nádrží   223 Technologická zařízení... <p>K jednotlivým grafickým vrstvám jsou připojeny specifické atributové záznamy</p>

4) Data:	Plochy pozemků a staveb ve správě TSK
Forma rozhraní pro předávání dat:	WMS
Frekvence aktualizace dat:	Kvartálně
Popis předávaných dat:	Data budou obsahovat zakres rozsahu, včetně popisných informací, jako je: <ul style="list-style-type: none"> ○ typ ○ vlastnictví ○ správa ○ GID