

Bezpečnostní opatření pro smluvní vztahy

1. ÚVOD

Tato příloha Smlouvy popisuje bezpečnostní požadavky projektu „Informační systém mezinárodní ochrany (IS AZYL III)“ zejména pro naplnění požadavků vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“), a vyhlášky 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 (dále jen „VyKB“), pro významný informační systém resortu MV.

2. BEZPEČNOSTNÍ POŽADAVKY

2.1. Účel

1. Tato příloha Smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro Zhotovitele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Objednatелеm a Zhotovitelem. Požadavky na Zhotovitele jsou definovány dle platné právní úpravy, především pak dle ZoKB, VyKB a zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „ZISVS“).
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZoKB, VyKB, ZISVS, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek Smlouvy zohledňující takové požadavky.

2.2. Obecné bezpečnostně provozní požadavky

Zhotovitel se při poskytování plnění pro Objednatel zavazuje plnit následující povinnosti:

1. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro Zhotovitele, jakožto budoucího významného dodavatele významného informačního systému, ze ZoKB, VyKB a ZISVS a reflektovat případné novely dotčených právních předpisů či novou právní úpravu, a bezpečnostními politikami stanovenými systémem řízení bezpečnosti informací (ISMS) Objednatel dle specifikace předmětu veřejné zakázky;
2. jmenovat nejpozději do tří pracovních dnů po dni účinnosti Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze Smlouvy a této přílohy a související komunikace mezi smluvními stranami (dále také jen „Kontaktní osoba pro bezpečnost na straně Zhotovitele“). Kontaktní osobu pro bezpečnost na straně Zhotovitele sdělí písemně Objednateli v téže lhůtě;
3. zajistit, aby Kontaktní osoba pro bezpečnost na straně Zhotovitele nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění této Smlouvy za stranu Zhotovitele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito Bezpečnostními požadavky;

4. minimálně 1x ročně provádět identifikaci a hodnocení aktiv a rizik významného informačního systému, která je součástí dodávaného řešení a na základě výsledků navrhopat a předkládat Objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik. Opatření musí být navrhována a konsolidována s přihlédnutím k výsledkům posuzování rizik i z hlediska dopadu na práva a svobody subjektů údajů.
5. dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Zhotoviteli Objednatelem, k jejímž dodržování se Zhotovitel zavázal, pokud byl Zhotovitel 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 Zhotoviteli, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu Zhotoviteli na sdílené úložiště aj.); vymezení relevantní části centrální dokumentace ISMS, která byla předána Zhotoviteli, je uveden v příloze č. 10 Smlouvy.
6. rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se podílejí na plnění Smlouvy a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci a další osoby na straně Zhotovitele podílející se na plnění Smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Objednatele, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro Objednatele v souvislosti s plněním této Smlouvy;
7. zaznamenávat a na vyžádání Objednateli poskytnout veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.);
8. přidělovat svým jednotlivým pracovníkům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele;
9. garantovat dostupnost, důvěrnost plnění a integritu předávaných dat s tím, že dodávané služby musí být v souladu s uzavřeným smluvním vztahem provozně monitorovány a vyhodnocovány;
10. průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Zhotovitele, které přistupují k předmětu plnění dle této Smlouvy;
11. zavést opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelně (alespoň 1x za čtvrtletí, vždy ale s minimálně dvouměsíčním odstupem) testovat funkčnost těchto záloh;
12. průběžně detekovat, minimálně však jednou za 3 měsíce, technické zranitelnosti a konfigurační nesoulady předmětu plnění Smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat Objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Zhotovitele. Nápravná opatření musí být schválena Objednatelem;
13. zajistit rozhraní pro napojení na dohledová centra Objednatele a součinnost při zvládnutí kybernetických bezpečnostních událostí a incidentů;

14. uchovávat data o provozu (provozní a lokalizační údaje) v souladu s požadavky účinné legislativy ČR a dodržovat požadavky VyKB na obsah provozních událostí.

2.3. Oprávnění užívat data

1. Zhotovitel je při poskytování plnění pro Objednatele oprávněn nakládat s daty předanými Zhotoviteli Objednatelem výhradně za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
2. Zhotovitel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.

2.4. Kontrola souladu s požadavky bezpečnosti

1. Zhotovitel je srozuměn s prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany Objednatele v souvislosti s poskytovanou službou Zhotovitelem.
2. Hodnocení, kontrola a audit probíhají v intervalech stanovených Objednatelem nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. Kontrola nebo audit mohou být provedeny v prostorách Zhotovitele nebo jeho poddodavatele a Zhotovitel má povinnost tyto kontroly a audity Objednateli či Objednatelem pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout Objednateli či Objednatelem pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Zhotoviteli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.
3. Zhotovitel je povinen po zavedení opatření provést také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Objednatelem, na žádost Objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá Zhotovitel Objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

2.5. Řetězení a řízení dodavatelů

Zhotovitel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1. Zhotovitel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení Objednatele;
2. Zhotovitel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů;
3. Zhotovitel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení;

4. Pokud Zhotovitel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Smlouvy. Zhotovitel se zavazuje bezodkladně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této Smlouvy;
5. Zhotovitel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele Zhotovitele, považuje se každé takové nedodržení požadavků za porušení povinnosti Zhotovitele dle této Smlouvy;

2.6. Povinnosti v řízení změn dle ZoKB a VyKB

1. Zhotovitel se zavazuje v rozsahu předmětu plnění aktivně podílet na splnění povinností v oblasti řízení změn dle ZoKB a VyKB, zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
2. Zhotovitel se minimálně zavazuje v rozsahu předmětu plnění na své straně přiměřeně reagovat na změny a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
3. Zhotovitel se zavazuje aktivně spolupracovat při testování významné změny.

2.7. Zvládání bezpečnostních událostí a incidentů

Zhotovitel se při poskytování plnění pro Objednatele zavazuje, že:

1. stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsanych pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů Objednatele, v případech, kdy situace nestrpí odklad telefonicky. Dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých nápravných opatřeních nad všemi částmi řešení, které jsou ve správě Zhotovitele, a rizicích souvisejících s ohrožením kontinuity činností vést záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Objednatele a legislativy ČR. Nastavená pravidla a postupy podléhají schválení Objednatelem;
2. nastavená pravidla pro zvládání bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získání musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;
3. navrhne řešení tak, aby byl systém detekce a zvládání bezpečnostních událostí a incidentů začleněn do procesů a systémů a realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti;

4. zajistí rozhraní pro napojení na dohledová centra Objednatele pro zvládání kybernetických bezpečnostních událostí a incidentů a zajistí součinnost a bude se řídit jeho pokyny;
5. provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Zhotovitel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2.8. Informační povinnost a povinnosti při výměně informací

1. Zhotovitel se během poskytování plnění pro Objednatele zavazuje Objednatele informovat o:
 - a) způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;
 - b) významné změně ovládnutí Zhotovitele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Zhotovitelem k plnění na základě smluvního vztahu s Objednatelem.
2. Zhotovitel se během poskytování plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost před hrozbami v kybernetické bezpečnosti v souladu s ZoKB a VyKB.

2.9. Specifikace podmínek pro řízení kontinuity činností a zálohování a obnovu dat z pohledu ZoKB a VyKB

1. Zhotovitel se zavazuje zpracovat plán řízení KBI a plán kontinuity a obnovy činností souvisejících s provozem řešení a všech jeho komponent na základě Zhotovitelem zpracovaného zhodnocení a výsledků z analýzy dopadů (Business Impact Analysis), která musí být schválena Objednatelem.
2. Zhotovitel se zavazuje dodržovat požadavky Objednatele na řízení kontinuity činností v souladu s ZoKB, VyKB a ustanoveními bezpečnostní politik, metodik a postupů předaných Zhotoviteli Objednatelem.
3. Zhotovitel vypracuje a předá Objednateli metodiku zálohování a obnovy dat (ve smyslu primárních aktiv) i systémů (resp. technických aktiv) ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována. Zhotovitel jako součást dodávky dále dodá a nasadí odpovídající technologické řešení, na kterém bude záloha a obnova dat prováděna. Toto řešení musí být nasazeno v primární i záložní lokalitě.
4. Plán řízení KBI, plán kontinuity a obnovy činností a metodika zálohování a obnovy dat i systémů musí být zpracovány nejpozději v rámci etapy 6 Díla.

2.10. Bezpečnost lidských zdrojů

1. Zhotovitel připraví poučení a zajistí poučení všech stran podílejících se na poskytování předmětu plnění dle Smlouvy o bezpečnostních pravidlech, jež se musí v průběhu dodávky dodržovat a zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů. Rozsah poučení podléhá schválení Objednatele.

2. Zhotovitel se zaváže zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávky, zastupitelnost pracovníků, zejména Kontaktní osoba pro bezpečnost na straně Zhotovitele).

2.11. Požadavky na systémovou a provozní bezpečnostní dokumentaci

1. Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace a dále také zpracování provozní dokumentace. Tato dokumentace musí být v souladu se ZoKB a VyKB.
2. V rámci poskytovaného plnění se Zhotovitel zavazuje Objednateli předat následující dokumentaci k řešení dle platné legislativy a dle požadavků Objednatele:
 - a) Bezpečnostní dokumentace významného informačního systému:
 - i. bezpečnostní politika,
 - ii. bezpečnostní směrnice pro činnost bezpečnostního správce systému,
 - iii. bezpečnostní a provozní postupy definující požadavky, procesní pravidla, role a odpovědnost v rámci jednotlivých procesů v rámci celého životního cyklu IS (od zajištění vývoje a rozvoje nových funkcí IS, následného předání do provozu, provozování a správy IS, nebo zařízení v produkci až po jeho vyřazení z používání).
 - b) Systémová příručka obsahující:
 - i. popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v informačním systému veřejné správy a návod na používání těchto funkcí,
 - ii. parametry kvality vycházejí z požadavků na kvalitu,
 - iii. podrobný popis IS nebo odkaz na dokument, ve kterém je popis uveden a který je Objednateli dostupný,
 - iv. popis jednotlivých činností vykonávaných při správě IS, včetně činností definovaných pro role, určení fyzických osob, které tyto činnosti vykonávají a oprávnění nezbytných pro výkon těchto činností,
 - v. definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání IS.
 - c) Uživatelská příručka obsahující:
 - i. popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost v IS a návod na použití těchto funkcí,
 - ii. vymezení oprávnění a povinností uživatelů ve vztahu k IS.
 - d) Dokumentace k integraci řešení, a to včetně identifikovaných datových toků, protokolů, architektonického nákresu komponent a jejich spolupráce, diagram logického a fyzického zapojení.
 - e) Další dokumentaci dle požadavku Objednatele.

- f) Zhotovitel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli také provozní dokumentaci v obdobném rozsahu dle předmětu a povahy Smlouvy:
- i. dokumentaci strategie obnovy,
 - ii. dokumentaci skutečného provedení,
 - iii. dokumentaci obsahující popis autorizačního konceptu a oprávnění,
 - iv. dokumentaci obsahující zálohovací a archivační postupy,
 - v. dokumentaci obsahující instalační a konfigurační postupy,
 - vi. dokumentaci obsahující bezpečnostní nastavení související s předmětem plnění smlouvy;

dále jen souhrnně „**Bezpečnostní a provozní dokumentace**“.

3. Bezpečnostní a provozní dokumentace musí být vytvořena dle poskytnutých šablon v rámci etapy 6 Díla.
4. Bezpečnostní a provozní dokumentace uvedená výše bude Objednateli Zhotovitelem předána nad rámec případné jiné předávané dokumentace vymezené v této Smlouvě.

2.12. Fyzická ochrana a bezpečnost prostředí

1. Zhotovitel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče (dále také jen „**Pracoviště**“).
2. Zhotovitel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění dle této Smlouvy.

2.13. Požadavky na Řízení přístupu

1. Zhotovitel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze konkrétním fyzickým osobám / zaměstnancům Zhotovitele / poddodavatele Zhotovitele zaevidované, a to na základě požadavku Zhotovitele na přístup.
2. Zhotovitel bere na vědomí, že přidělení oprávnění zaměstnanci Zhotovitele musí být řízeno zásadou tzv. „potřeba vědět“ (need-to-know principle) a není nárokové.
3. Zhotovitel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Zhotovitele nebo poddodavatele Zhotovitele.
4. Zhotovitel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Objednatelem.
5. Zhotovitel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Zhotovitel bere na vědomí, že přístup do interní sítě Objednatele a/nebo k technologickým a komunikačním systémům Objednatele bude realizován výhradně s využitím zařízení Objednatele.

6. Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Objednatele. Zhotovitel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídicí dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Zhotovitele, pokud byl s takovou řídicí dokumentací Objednatele seznámen).
7. Zhotovitel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnosti vzniklé v důsledku porušení Bezpečnostních požadavků nebude posuzována jako okolnost vylučující odpovědnost Zhotovitele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Zhotoviteli či jiné osobě ze strany Zhotovitele. Ostatní ustanovení ohledně odpovědnosti Zhotovitele za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.

2.14. Monitorování činností

1. Zhotovitel bere na vědomí, že veškerá aktivita Zhotovitele a jeho plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související budou Objednatelům průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Objednatele.
2. Zhotovitel se zavazuje, že bude průběžně monitorovat a zaznamenávat veškerou svoji aktivitu a plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související. Zhotovitel je povinen předkládat Objednateli záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ICT systému a záznamy o správě uživatelů prováděná na straně Zhotovitele, a to v pravidelných intervalech dle sjednaného harmonogramu, nebo kdykoli bez zbytečného odkladu po vyžádání ze strany Objednatele, a to po celou dobu trvání Smlouvy a i ve vztahu k jejímu ukončení.

2.15. Předání a převzetí plnění

1. Zhotovitel se zavazuje dodržovat Bezpečnostní požadavky i při předání a převzetí plnění dle této Smlouvy
2. Objednatel je oprávněn z důvodu nedodržení Bezpečnostních požadavků včetně požadavku na předání Bezpečnostní dokumentace odmítnout převzetí (části) plnění Smlouvy.

2.16. Likvidace dat

Zhotovitel se zavazuje plnit požadavky Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů dat) dle přílohy č. 4 VyKB.

2.17. Sankce

Sankce za porušení povinností plynoucích z bezpečnostních opatření a ZoKB a VyKB jsou uvedeny v hlavním textu Smlouvy.

2.18. Způsob distribuce dokumentů Objednateli

Zhotovitel má právo vyžádat si od Objednatele shora uvedené dokumenty vymezené v Příloze č. 10 Smlouvy, které mu budou předány na základě Dohody o zachování mlčenlivosti o důvěrných informacích (NDA).

