Příloha č. 3 Smlouvy o technické podpoře

Kybernetická bezpečnostní opatření zohledňující specifické požadavky plynoucí ze zajištění provozních a bezpečnostních potřeb souvisejících s regulovanou službou

Objednatel, který je poskytovatelem regulované služby v režimu nižších povinností podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti"), je povinen při zavádění a provádění bezpečnostních opatření, která jsou přiměřená jeho bezpečnostním potřebám, zajistit při uzavírání smlouvy s dodavatelem požadavky ve stanoveném rozsahu podle § 12 zákona o kybernetické bezpečnosti, zohlednit hrozby a zranitelnosti spojené s dodavatelem, celkovou kvalitu produktů, služeb a postupů v oblasti kybernetické bezpečnosti dodavatele, a dále zajistit, aby smlouva obsahovala relevantní smluvní ujednání uvedené v příloze č. 2 vyhlášky č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „vyhláška o bezpečnostních opatřeních v režimu nižších povinností"). Proto může objednatel uzavírat pouze takové smlouvy, které stanoví konkrétní způsoby realizace bezpečnostních opatření a určují obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu takových bezpečnostních opatření.

Z těchto důvodů je poskytovatel povinen při poskytování služeb dodržovat pro potřeby zajištění kybernetické bezpečnosti následující povinnosti, a to vždy v rozsahu přiměřeném povaze, rozsahu a rizikovosti poskytovaného plnění:

Pro účely této přílohy smlouvy se smlouvou rozumí smlouva, jejíž je tato příloha součástí (dále jen „smlouva").

Čl. I
Požadavky na kybernetickou bezpečnost

1. Poskytovatel se zavazuje plnit povinnosti stanovené touto přílohou a postupovat tak, aby objednateli umožnil splnit jeho povinnosti podle zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních v režimu nižších povinností, zejména:

   a) **Bezpečnost informací a dat:** Při poskytování služby je poskytovatel povinen zavést a udržovat veškerá potřebná technická a organizační opatření k zajištění bezpečnosti informací a dat. Poskytovatel zejména zajistí, aby informace a data:

      (i) byly chráněny před neoprávněným zpřístupněním či zveřejněním (důvěrnost),
      (ii) byly chráněny před neoprávněnými změnami, poškozením nebo ztrátou (integrita), a
      (iii) zůstaly objednateli dostupné v souladu s podmínkami smlouvy (dostupnost).

      Za tím účelem se poskytovatel zavazuje dodržovat přiměřené bezpečnostní standardy a postupy, zejména se zavazuje:

      (i) zajistit bezpečnost softwaru a služby,
      (ii) dodržovat přijatá bezpečností opatření na ochranu informací a dat, zejména:
         - informace a data vložená objednatelem do softwaru nebo služby chránit šifrováním v rozsahu odpovídajícím povaze dat a rizikům zpracování,
         - zabezpečit veškerou komunikaci aktuálně odolným protokolem (nejméně SSL zejména však TLS ve verzi 1.2 nebo vyšší, není-li s ohledem na konkrétní službu sjednáno jinak),
         - omezit přístup k serverům, administrátorským rozhraním a jiným technickým aktivům pouze na oprávněné osoby a nezbytný rozsah (vzdálený administrátorský přístup umožnit pouze prostřednictvím zabezpečeného připojení, zejména VPN nebo rovnocenného mechanismu schváleného objednatelem),
         - pravidelně informace a data zálohovat a tyto zálohy bezpečně ukládat způsobem umožňujícím jejich obnovu,
         - informace a data v elektronické podobě uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým budou mít přístup pouze pověřené osoby na základě jednoznačně přiřazených přístupových oprávnění (kódů či hesel),
         - zajistit vzdálený přenos informací a dat buď pouze prostřednictvím veřejně nepřístupné sítě (VPN), nebo prostřednictvím zabezpečeného přenosu po veřejných sítích,

(iii) pro ochranu komunikace používat pouze takové části segmentované sítě objednatele nebo jeho služby, které poskytovatel nezbytně potřebuje k plnění podle smlouvy, omezit komunikaci na perimetru na nezbytný rozsah a dobu, a používat aktuálně odolné a bezpečné komunikační protokoly,

(iv) vzdálené přístupy zabezpečit tak, aby byla zajištěna důvěrnost a integrita informací a dat; poskytovatel je povinen používat po celou dobu trvání smlouvy VPN tunel nebo jiné metody vzdáleného přístupu, monitoring činností, PAM systém, je-li to s ohledem na rozsah oprávnění přiměřené, aktuálně odolné kryptografické algoritmy, zohledňovat metodiky a doporučení NÚKIB a zajišťovat bezpečnou e-mailovou, hlasovou i textovou komunikaci,

(v) pravidelně a bez zbytečného odkladu aplikovat bezpečnostní aktualizace, zejména aktualizace odstraňující zranitelnosti se závažným nebo kritickým dopadem,

(vi) pravidelně provádět skenování zranitelností, vyhodnocovat zjištěné zranitelnosti podle jejich závažnosti a přijímat přiměřená nápravná opatření,

(vii) o informacích a datech zachovávat mlčenlivost a chránit jejich důvěrnost, zejména nepoužít informace a data pro jiné účely než ve smlouvě uvedené a bez předchozího písemného souhlasu objednatele nezpřístupnit informace a data třetím osobám,

(viii) zajistit, aby jakákoliv fyzická osoba, která jedná z pověření poskytovatele (zejména zaměstnanec poskytovatele nebo subdodavatele), která má přístup k informacím a datům, byla vázána povinností mlčenlivosti, poučena o povinnostech poskytovatele dle této přílohy smlouvy a řádně proškolena v ochraně důvěrných informací,

(ix) zajistit integritu a dostupnost informací a dat, a za tímto účelem vést přiměřené záznamy umožňující ověřit plnění těchto povinností.

b) **Audit a kontrola:** Objednatel má právo provést kontrolu a audit poskytovatele související s plněním podle smlouvy, zejména dodržování sjednaných bezpečnostních opatření uvedených v této příloze smlouvy, a to i prostřednictvím k tomu sjednané třetí osoby, která není v přímém střetu zájmů a je vázána mlčenlivostí. Poskytovatel umožní audit na základě přiměřeného předchozího oznámení; v případě kybernetického bezpečnostního incidentu, významné hrozby nebo důvodného podezření na porušení této přílohy smlouvy umožní audit bez zbytečného odkladu. Pro potřeby auditu poskytne všechny relevantní informace související s plněním podle smlouvy, a to i o činnostech svých subdodavatelů, kteří se případně podílejí na plnění podle smlouvy. Náklady na provedení auditu nese objednatel, není-li audit vyvolán podstatným porušením povinností poskytovatele, v takovém případě nese přiměřené náklady auditu poskytovatel. Poskytovatel se zavazuje poskytnout při auditu veškerou potřebnou součinnost, zejména umožnit přístup k relevantním záznamům, systémům a zařízením, poskytnout logy a odpovědět na dotazy auditorů, vždy však v rozsahu přiměřeném účelu auditu a při zachování bezpečnosti a důvěrnosti informací ostatních zákazníků poskytovatele. Pokud audit odhalí nedostatky v plnění povinností poskytovatele v rámci bezpečnostních opatření dle této přílohy smlouvy, poskytovatel je povinen tento stav bez zbytečného odkladu napravit a písemně o nápravě informovat objednatele.

c) **Řetězení dodavatelů:** Poskytovatel může zapojit subdodavatele pouze s předchozím písemným souhlasem objednatele. Poskytovatel je povinen zajistit, aby každý schválený subdodavatel byl smluvně zavázán k dodržování povinností v rozsahu odpovídajícím povinnostem poskytovatele podle této přílohy smlouvy, zejména pokud jde o bezpečnost informací, ochranu dat, mlčenlivost, součinnost při auditu, řešení kybernetických bezpečnostních incidentů a exit strategii. Objednatel je oprávněn stanovit podmínky a kritéria pro výběr subdodavatele (např. požadavek určité bezpečnostní certifikace) a může ze závažných důvodů již schváleného subdodavatele kdykoli odmítnout nebo odvolat svůj souhlas. I v případě písemného odsouhlasení subdodavatele objednatelem odpovídá poskytovatel za plnění povinností podle smlouvy a podle této přílohy smlouvy tak, jako by plnil závazky sám.

d) **Exit strategie:** V případě ukončení smlouvy je poskytovatel povinen realizovat bezpečný ukončovací proces s cílem ochránit informace a data objednatele. Poskytovatel nejpozději do třiceti (30) dnů od ukončení smlouvy předá objednateli veškeré informace a data, podklady, dokumentaci a zálohy nezbytné k zajištění kontinuity provozu, a to v běžně a strojově čitelném použitelném elektronickém formátu podle pokynů objednatele. Poskytovatel předá rovněž přístupové údaje, klíče, certifikáty nebo jiné autentizační prostředky, které je oprávněn předat a které jsou nezbytné k převzetí nebo migraci služby. Předání bude potvrzeno protokolem podepsaným oběma stranami. Zároveň poskytovatel bezpečným způsobem vymaže nebo zničí všechny kopie těchto informací a dat ve svých systémech a nosičích, ledaže jejich další uchování vyžadují právní předpisy nebo je nezbytné pro uplatnění právních nároků; v takovém případě je zabezpečí a ponechá pouze po nezbytnou dobu bez možnosti jiného využití. Poskytovatel dále zruší účty a přístupová oprávnění zřízená pro plnění smlouvy, zejména oprávnění svých pracovníků a subdodavatelů k systémům objednatele, a provede další nezbytné kroky k ukončení poskytování služby tak, aby nebyla ohrožena bezpečnost informací a dat poskytovatele. V případě požadavku na migraci ze strany objednatele, je poskytovatel

povinen poskytnout nezbytnou součinnost (např. exporty ze systémů a databází nebo předání provozní dokumentace).

e) **Oprávnění používat data:** Poskytovatel se zavazuje užívat informace, data a jiné podklady, ke kterým získal přístup v rámci plnění podle smlouvy, pouze k naplnění svého závazku sjednaného v předmětu nebo účelu podle smlouvy. Objednateli náleží veškerá práva a oprávněné zájmy k informacím a datům, která mu náležela před jejich předáním poskytovateli, nebo která pro něj vznikla při plnění smlouvy; poskytovatel k nim nenabývá žádné vlastnické ani jiné právo, není-li výslovně sjednáno jinak. Poskytovatel má po dobu trvání smlouvy právo tyto informace a data užívat pouze v rozsahu nezbytném pro řádné poskytování služby a plnění svých povinností podle smlouvy. Poskytovatel nesmí tyto informace a data využít k žádnému jinému účelu, zejména je bez předchozího písemného souhlasu objednatele nesmí zpřístupnit či poskytnout třetí osobě, ani je použít pro vlastní potřebu. Poskytovatel je zejména povinen:

   (i) zavést bezpečnostní opatření k zajištění, aby k těmto informacím a datům měly přístup pouze osoby pověřené plněním podle smlouvy, zejména je povinen zajistit, že informace a data v elektronické podobě budou uchovávány na zabezpečených serverech nebo na nosičích dat, ke kterým budou mít přístup pouze pověřené osoby na základě jednoznačně přiřazených přístupových oprávnění (kódů či hesel),
   (ii) v souladu s čl. II této přílohy smlouvy o informacích a datech zachovávat mlčenlivost a chránit jejich důvěrnost, zejména nepoužít informace a data, pro jiné účely než ve smlouvě uvedené a bez předchozího písemného souhlasu objednatele je nezpřístupnit třetím osobám,
   (iii) zajistit, aby jakákoliv fyzická osoba, která jedná z pověření poskytovatele (zejména zaměstnanec poskytovatele nebo subdodavatele), která má přístup k informacím a datům, byla vázána povinností mlčenlivosti, poučena o povinnostech poskytovatele dle této přílohy smlouvy a řádně proškolena v ochraně důvěrných informací,
   (iv) po ukončení smlouvy naložit s informacemi a daty způsobem stanoveným v písm. d) tohoto odstavce.

f) **Autorství programového kódu/programové licence:** Není-li ve smlouvě výslovně sjednáno jinak, poskytovatel prohlašuje, že je oprávněn k poskytování služby a že má k používanému softwaru veškerá práva potřebná k plnění smlouvy a že výkonem práv a povinností podle smlouvy nedojde k porušení práv duševního vlastnictví žádné třetí osoby. Na základě smlouvy uděluje poskytovatel objednateli právo k užívání softwaru ve sjednaném rozsahu, a to nejméně po dobu trvání smlouvy nebo na dobu potřebnou k naplnění účelu smlouvy. Poskytovateli zůstávají práva k programovému kódu, struktuře a architektuře softwaru, algoritmům, know-how metodikám automatizace a jednotlivým procesům, pokud smlouva nestanoví, že konkrétní výstup nebo jeho část náleží objednateli.
   Poskytovatel se zavazuje zajistit, že jakékoliv užití komponent třetích stran, včetně open-source komponent v rámci poskytované služby bude vždy v souladu s licenčními podmínkami třetích stran a nebude omezovat sjednané užívání služby objednatelem. Pokud vůči objednateli uplatní třetí osoba jakýkoliv nárok z titulu porušení práv duševního vlastnictví v souvislosti s užíváním softwaru, zavazuje se poskytovatel na své náklady zajistit mimosoudní vyřešení takové situace, poskytnout objednateli nezbytnou součinnost a v případě vzniku škody nebo jiné újmy objednatele tuto škodu nebo újmu nahradit v rozsahu stanoveném právními předpisy a smlouvou.

g) **Řízení změn:** Poskytovatel se zavazuje uplatňovat kontrolovaný proces řízení změn při takových podstatných změnách služby, softwaru (včetně architektury softwaru), hardwaru, konfigurace, umístění zpracování nebo zapojení subdodavatelů, které by mohly ovlivnit bezpečnost zpracování informací a dat, dostupnost služby nebo plnění povinností objednatele podle právních předpisů (dále jen „podstatné změny"), a zároveň se zavazuje zajistit, že žádná taková podstatná změna nepovede k nepřiměřenému narušení plynulosti provozu služby ani ke snížení úrovně její bezpečnosti. Poskytovatel se dále zavazuje:

   (i) podstatné změny konfigurace a provozních parametrů služby, které mohou mít dopad na bezpečnost, dostupnost nebo interoperabilitu služby, softwaru nebo hardwaru provádět pouze po předchozím oznámení objednateli a po jeho schválení, vyžaduje-li to smlouva nebo povaha podstatné změny,

   (ii) při aktualizacích jakýkoliv součásti systémů, změnách softwaru nebo konfigurace zařízení, případně při reinstalaci nebo náhradě softwaru nebo hardwaru, užívat pouze software, k němuž má poskytovatel potřebné oprávnění a který neomezuje oprávněné užívání na služby,

   (iii) všechny plánované podstatné změny služby, softwaru nebo hardwaru oznámit objednateli písemně e-mailem alespoň pěti (5) pracovních dnů předem, není-li ve smlouvě sjednána lhůta jiná, a poskytnout popis navrhované změny spolu s posouzením jejího předpokládaného dopadu na bezpečnost, dostupnost a kontinuitu služby.

V naléhavých případech, kdy je nutné neprodleně provést podstatnou změnu za účelem odvrácení hrozícího kybernetického bezpečnostního incidentu nebo odstranění závažné zranitelnosti softwaru, je poskytovatel oprávněn provést nezbytnou podstatnou změnu i bez předchozího souhlasu objednatele; o takové podstatné změně však informuje objednatele bez zbytečného odkladu poté, co ji provede, a dodatečně poskytne popis provedené podstatné změny, důvody jejího urgentního provedení a vyhodnocení jejích dopadů.

h) **Kybernetické bezpečnostní hrozby, zranitelnosti a incidenty:** Poskytovatel je povinen neprodleně a bez zbytečného odkladu informovat objednatele o každé zjištěné kybernetické bezpečnostní významné hrozbě, zranitelnosti, události nebo incidentu, které mají nebo by mohly mít vliv na poskytování služby, integritu, důvěrnost, nebo dostupnost informačních systémů objednatele nebo bezpečnost informací a dat objednatele (dále jen „kybernetický bezpečnostní incident). Oznámení o kybernetickém bezpečnostním incidentu musí být učiněno nejpozději do 24 hodin od zjištění takového kybernetického bezpečnostního incidentu poskytovatelem a musí obsahovat dostupné informace o povaze kybernetického bezpečnostního incidentu, dotčených systémech, předpokládaných dopadech, o přijatých či plánovaných opatřeních k nápravě a kontaktní osobě poskytovatele pro řešení kybernetického bezpečnostního incidentu.

   (i) Poskytovatel neprodleně přijme veškerá přiměřená opatření k minimalizaci dopadů takového kybernetického bezpečnostního incidentu, k obnovení bezpečného provozu služby nebo softwaru a k zamezení opakování obdobných kybernetických bezpečnostních incidentů.

   (ii) Poskytovatel poskytne objednateli plnou součinnost při řešení a vyšetřování kybernetického bezpečnostního incidentu, včetně umožnění přístupu k relevantním logům, systémům a dalším informacím potřebným k analýze příčin a následků, a to v rozsahu nezbytném pro splnění zákonných a smluvních povinností objednatele.

   (iii) V případě, že charakter kybernetického bezpečnostního incidentu zakládá povinnost učinit oznámení orgánům veřejné moci, Národnímu CERT, NÚKIB nebo jiným dotčeným osobám, je poskytovatel povinen spolupracovat s objednatelem tak, aby byly takové oznamovací povinnosti splněny v zákonem stanovených lhůtách. Poskytovatel nesmí bez předchozího souhlasu objednatele činit veřejná oznámení o incidentu, ledaže mu to ukládá právní předpis nebo rozhodnutí orgánu veřejné moci.

   (iv) O průběhu a závěrech řešení každého významného kybernetického bezpečnostního incidentu vyhotoví poskytovatel záznam nebo zprávu, kterou na vyžádání poskytne objednateli; zpráva musí přiměřeně popsat příčinu, rozsah, dopad, přijatá opatření, doporučená preventivní opatření a časovou osu řešení.

i) **Kontinuita činností:** Poskytovatel zajistí řízení kontinuity jím poskytovaných služeb v souladu s plněním podle smlouvy. Poskytovatel zavede a bude udržovat adekvátní opatření pro zajištění kontinuity svých činností a nepřerušeného poskytování služby i v případě mimořádných událostí, výpadků nebo jiných narušení provozu služby (dále jen „mimořádná událost"). V případě vzniku mimořádné události, jež způsobí omezení nebo přerušení provozu služby, je poskytovatel povinen neprodleně informovat objednatele o nastalé situaci a zajistit obnovení poskytování služby ve lhůtách sjednaných ve smlouvě (SLA); nejsou-li takové lhůty sjednány, v nejkratší přiměřené době s ohledem na povahu služby a závažnost mimořádné události.

   Poskytovatel je povinen zajistit pravidelné zálohování informací a dat objednatele zpracovávaných v rámci služby s frekvencí nejméně jednou denně, není-li ve smlouvě sjednána jiná přiměřená frekvence, a uchovávat tyto zálohy po dobu alespoň 6 měsíců, není-li ve smlouvě sjednána jiná doba. Záložní data musí být zabezpečena a uložena způsobem odděleným od primární infrastruktury služby tak, aby byla umožněna obnova regulované služby po mimořádné události.

j) **Úroveň služeb SLA:** SLA parametry (zejména dostupnost služby, reakční doby, doby odstranění vad, RTO, RPO, způsob eskalace, kontaktní místa, způsob a úroveň realizace bezpečnostních opatření) jsou sjednány ve smlouvě popřípadě ve zvláštní dohodě o SLA. Nejsou-li konkrétní SLA parametry sjednány, je poskytovatel povinen postupovat s odbornou péčí a obnovit poskytování služby bez zbytečného odkladu.

k) **Bezpečný vývoj:** Poskytovatel se zavazuje dodržovat pravidla bezpečného vývoje softwaru při veškerých činnostech vývoje, údržby a aktualizací, pokud jsou součástí plnění podle smlouvy. Poskytovatel zajistí, že jeho vývojový proces zahrnuje adekvátní kontrolní mechanismy k minimalizaci vzniku zranitelností, včetně průběžné analýzy zdrojového kódu z hlediska bezpečnosti, správy závislostí, využívání prověřených verzí komponent, evidence komponent třetích stran a provádění testů zranitelností před nasazením každé významné aktualizace služby. Tyto činnosti provádí poskytovatel v souladu s uznávanými standardy a osvědčenými postupy pro bezpečný vývoj softwaru, zejména přiměřeně podle metodik, a s požadavky a doporučeními NÚKIB (např. v dokumentu Bezpečnostní doporučení pro vývoj otevřeného softwaru ve veřejné správě), obdobných relevantní standardů a v souladu se zákonem o kybernetické bezpečnosti; totéž

platí i pro subdodavatele užívajícího software poskytovatele nebo pro software vytvořený subdodavatelem. Pokud je v provozované verzi služby zjištěna bezpečnostní chyba nebo zranitelnost, poskytovatel ji neprodleně odstraní nebo přijme přiměřené zmírňující opatření. Poskytovatel je dále povinen na požádání poskytnout objednateli informace o svém procesu testování a zajištění bezpečnosti softwaru a o bezpečnostních standardech, které při vývoji a provozu služby dodržuje.

l) **Dodržování bezpečnostní politiky:** Poskytovatel se zavazuje dodržovat veškeré bezpečnostní politiky objednatele, které mu objednatel předal nebo sdělil, a se kterými byl prokazatelně seznámen, a to v rozsahu, který je nezbytný pro plnění podle smlouvy a přiměřený povaze poskytované služby, především pak ve vztahu k zajištění bezpečnosti informací a dat v rámci provozu služby. Poskytovatel prohlašuje, že byl seznámen s bezpečnostní politikou dle předchozí věty v nezbytném rozsahu, což stvrzuje podpisem smlouvy; nebyla-li mu bezpečnostní politika předána, použijí se vlastní bezpečnostní politiky poskytovatele písemně odsouhlasené objednatelem nebo minimálně obvyklé bezpečnostní standardy odpovídající povaze plnění. Poskytovatel se zavazuje, řídit se po celou dobu trvání smlouvy vlastními bezpečnostními politikami uvedenými v smlouvě i bezpečnostními politikami objednatele dle předchozí věty, podle toho, které z nich zajišťují vyšší úroveň ochrany a bezpečnosti informací a dat; pokud jsou ve vzájemném rozporu, tak je poskytovatel povinen řídit se bezpečností politikou objednatele. Poskytovatel je povinen oznámit objednateli každou zamýšlenou změnu své bezpečnostní politiky, která by se mohla podstatně dotknout bezpečnosti poskytované služby pro objednatele, přičemž takovou změnu smí provést pouze tehdy, pokud nesníží sjednanou úroveň bezpečnosti, nebo s předchozím písemným souhlasem objednatele.

2. Pokud poskytovatel pro potřeby poskytování služeb bude potřebovat vzdálený přístup k dotčeným systémům objednatele, pak mu bude tento přístup umožněn za následujících podmínek:

   a) přístup bude umožněn pouze pracovníkům poskytovatele podle předloženého a průběžně aktualizovaného seznamu a poskytovatel je povinen zajistit, že tito pracovníci obdrží přidělené přístupové údaje v tajnosti a nebudou je sdílet s jinou osobou,

   b) dojde-li ke ztrátě přístupových údajů nebo k podezření na jejich prozrazení či zneužití, oznámí poskytovatel tuto skutečnost bez zbytečného odkladu kontaktní osobě objednatele pro otázky bezpečnosti informací,

   c) poskytovatel bude akceptovat přiměřené technologické požadavky objednatele, které se mohou v průběhu plnění smlouvy měnit (např. VPN tunel, vícefaktorová autentizace, monitoring činností poskytovatele, PAM systém) pokud jsou nezbytné pro zajištění bezpečnosti regulované služby a objednatel je poskytovateli oznámí v přiměřené lhůtě.

Čl. II
Ochrana důvěrných informací

1. Poskytovatel se zavazuje zachovávat mlčenlivost o skutečnostech týkajících se objednatele, o nichž se dozví v souvislosti s plněním předmětu smlouvy, jakož i o veškerých dalších skutečnostech a informacích, které byly nebo budou poskytovateli sděleny objednatelem, a které zároveň nejsou veřejně známé nebo dostupné, a o nichž lze zároveň důvodně předpokládat, že na jejich utajení má objednatel zájem (dále jen „důvěrné informace").

2. Všechny informace a údaje ke kterým získá poskytovatel přístup mají důvěrný charakter, a to i v případech, kdy je nelze považovat za obchodní tajemství ve smyslu § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník") nebo nejsou chráněny jiným právním předpisem.

3. Poskytovatel se rovněž zavazuje zachovávat mlčenlivost o skutečnostech a informacích, které objednatel výslovně označil za důvěrné informace, a to např. prostřednictvím poznámky „důvěrné", „tajné" či obdobně. Takto označené informace jsou považovány za důvěrné informace ve smyslu této přílohy smlouvy. Pro vyloučení pochybností se smluvní strany dohodly, že důvěrné informace není nutné výslovně označovat, avšak za účelem vyloučení pochybností o charakteru informací je jejich označení vhodné, a to zejména v případech, kdy by nemusel být charakter informací jednoznačně zřejmý.

4. Poskytovatel takové důvěrné informace neprozradí ani neposkytne žádné třetí osobě a nepoužije je pro jiný účel než pro plnění účelu smlouvy. Povinnost mlčenlivosti se nevztahuje na informace, které poskytovatel prokazatelně získal jinak než porušením smlouvy a které:

   a) jsou veřejně dostupné nebo se staly veřejně známými bez porušení smlouvy,

   b) musí být zpřístupněny na základě zákona nebo pravomocného rozhodnutí orgánu veřejné moci.

5. Při realizaci plnění podle smlouvy se nepředpokládá, že poskytovatel bude mít přístup k osobním údajům, u nichž je objednatel správcem, není-li ve smlouvě nebo v samostatné smlouvě o zpracování osobních údajů sjednáno jinak. Pokud bude poskytovatel pro objednatele zpracovávat osobní údaje, strany před zahájením takového zpracování uzavřou smlouvu o zpracování osobních údajů nebo jiné právní ujednání splňující požadavky čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR). Pokud se přesto poskytovatel nahodile dostane do styku s osobními údaji, platí pro tuto situaci ustanovení této části přílohy smlouvy o důvěrných informacích a poskytovatel je povinen o tom bez zbytečného odkladu informovat objednatele. Tím nejsou dotčeny povinnosti stran podle obecných právních předpisů o ochraně osobních údajů, především podle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR).

6. Při nakládání s důvěrnými informacemi sjednávají strany tyto závazky:

   a) Poskytovatel se zavazuje zajistit, aby nedošlo k úniku, zveřejnění a šíření důvěrných informací získaných od objednatele, a zavazuje se chránit tajnost důvěrných informací minimálně stejným způsobem, jakým chrání své obchodní tajemství, vždy však způsobem obvyklým pro ochranu obchodního tajemství.

   b) Poskytovatel se zavazuje vynaložit veškeré přiměřené úsilí, aby tajnost důvěrných informací byla důsledně dodržována i všemi osobami podílejícími se za poskytovatele na plnění smlouvy, především jeho zaměstnanci i případnými subdodavateli, které k plnění účelu spolupráce použije, pokud mu jejich použití objednatel v rámci plnění podle smlouvy umožní. Použije-li poskytovatel k plnění třetí osoby, je oprávněn zpřístupnit jí důvěrné informace získané od objednatele pouze v rozsahu nezbytně nutném pro jí poskytované plnění a je rovněž povinen zavázat třetí osobu povinností mlčenlivosti v rozsahu podle smlouvy. Za porušení povinností třetí osobou odpovídá poskytovatel.

   c) Poskytovatel je povinen zajistit, aby jeho zaměstnanci, kterým budou zpřístupněny důvěrné informace, byli v pracovněprávním nebo smluvním vztahu zavázáni dodržovat povinnosti odpovídající povinnostem dle ujednání tohoto článku přílohy smlouvy. Smluvní strany se zavazují omezit šíření důvěrných informací či údajů pouze na ty zaměstnance a další pověřené osoby, které se musí přímo podílet na vzájemné spolupráci smluvních stran.

   d) Poskytovatel se zavazuje nakládat s důvěrnými informacemi získanými od objednatele výlučně pro napění účelu smlouvy, a nikoliv pro jakýkoliv jiný účel.

   e) Poskytovatel odpovídá za nedbalostní i úmyslné sdělení nebo užití důvěrných informací a za škodu nebo jinou újmu z toho vzniklou dle § 2894 a násl. občanského zákoníku.

   f) Pokud by došlo k situaci, u které lze důvodně předpokládat ohrožení ochrany důvěrných informací, zavazuje se poskytovatel oznámit tuto skutečnost objednateli bez zbytečného odkladu. Pokud by objednatel pojal důvodné podezření, že poskytovatel není schopen zabezpečit ochranu důvěrných informací podle této přílohy smlouvy, je oprávněn požádat poskytovatele o to, aby prokázal plnění povinností podle této přílohy smlouvy a poskytovatel této žádosti vyhoví v přiměřené lhůtě.

   g) Poskytovatel je povinen po ukončení plnění podle smlouvy veškeré nosiče, na kterých jsou případně důvěrné informace zachyceny, neprodleně předat objednateli nebo je bezpečně zničit, ledaže právní předpis vyžaduje jejich další uchování.

7. Poskytovatel bere na vědomí, že jeho závazky k ochraně informací a mlčenlivosti dle ujednání v tomto článku této přílohy smlouvy trvají pod dobu 10 let po zániku smlouvy, ve vztahu k obchodnímu tajemství, informacím významným pro kybernetickou bezpečnost a informacím, jejichž zveřejnění by mohlo ohrozit bezpečnost objednatele nebo třetích osob, trvají po dobu, po kterou mají tyto informace důvěrnou povahu.

8. Následující kontaktní osoby jsou odpovědné za správu a administraci, včetně předávání či přijímání důvěrných informací dle této přílohy smlouvy:

   - za poskytovatele: Ing. Radek Černobila, tel. [redacted] email [redacted]

   - za objednatele: Mgr. René Rozsypal, tel. [redacted] email: [redacted]

9. Každá ze smluvních stran je oprávněna změnit své kontaktní osoby písemným oznámením druhé smluvní straně. Předávané důvěrné informace jsou chráněny podle této přílohy smlouvy, i když nejsou předávány kontaktními osobami nebo kontaktním osobám.

Čl. III
Sankce za porušení smluvních povinností

1. Poruší-li poskytovatel některou z povinností ujednanou **v čl. I odst. 1 písm. a), c), d), e), h), k), l) a písm. g) s výjimkou bodu (ii), v čl. I odst. 2 a v čl. II odst. 1, 2, 3, 4, 6 a 7** této přílohy smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši **100 000 Kč** za každý případ porušení takové smluvní povinnosti, není-li ve smlouvě sjednána jiná výše nebo způsob určení smluvní pokuty přiměřený hodnotě a rizikovosti plnění.
2. Poruší-li poskytovatel některou z povinností ujednanou **v čl. I odst. 1 písm. b), f), i) a j) a písm. g) bodu (ii) a v čl. II odst. 5** této přílohy smlouvy, je povinen zaplatit objednateli smluvní pokutu ve výši **25 000 Kč** za každý případ porušení takové smluvní povinnosti, není-li ve smlouvě sjednána jiná výše nebo způsob určení smluvní pokuty přiměřený hodnotě a rizikovosti plnění.
3. Smluvní pokuty jsou splatné do třiceti (30) dnů ode dne doručení písemné výzvy k úhradě, pokud ve výzvě není uvedena lhůta delší, a to způsobem uvedeným ve výzvě.
4. Ujednáním o smluvních pokutách není dotčeno právo poškozeného objednatele na náhradu škody nebo jiné újmy v plné výši, přičemž za škodu se považuje i ušlý zisk; nárok na náhradu nemajetkové újmy tím není dotčen, pokud jej lze podle právních předpisů uplatnit.

Čl. IV
Závěrečná ustanovení

1. Povinnosti poskytovatele stanovené v této příloze smlouvy se uplatní přiměřeně s ohledem na charakter, rozsah, předmět a rizikovost poskytované služby či jiného plnění a s ohledem na účel smlouvy, a to především na základě jejich přiléhavosti a proveditelnosti. V případě pochybností, zda se konkrétní ustanovení této přílohy smlouvy použije (včetně případného rozsahu jeho přiměřené aplikace), anebo zda se na poskytovanou službu či jiné plnění nepoužije z důvodu své zjevné nepřiléhavosti, neproveditelnosti nebo zjevné nepřiměřenosti, rozhoduje výlučně objednatel. Tím nejsou dotčeny povinnosti poskytovatele vyplývající ze smlouvy a z obecně závazných právních předpisů.
2. V případě, že úprava obsažená v této příloze smlouvy bude v rozporu s ustanovením smlouvy, smluvní strany se dohodly, že přednost má úprava dle této přílohy smlouvy, ledaže smlouva obsahuje výslovné zvláštní ujednání pro konkrétní plnění, které poskytuje alespoň srovnatelnou úroveň kybernetické bezpečnosti a není v rozporu s kogentními právními předpisy. Výklad smlouvy a této přílohy smlouvy musí směřovat k naplnění požadavků kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních v režimu nižších povinností.
3. Tato příloha smlouvy zůstane v platnosti i po ukončení smlouvy, a to až do doby, než dojde k řádnému předání nebo likvidaci všech informací a dat objednatele, s výjimkou čl. II této přílohy smlouvy, jehož zvláštní ustanovení o trvání je obsaženo v odst. 7 téhož článku této přílohy smlouvy.