Příloha č. 2 - Bezpečnostní požadavky a opatření

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 ovládání 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 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
- bezpečností 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 uchovávání 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.

**pro účely Přílohy č. .. se Objednatelem rozumí ……, Dodavatelem se rozumí ……*