NÚKIB

POŽADAVKY NA SMLOUVY S DODAVATELI

Verze 1.1, platná ke dni 29. 1. 2019

Úvod

Tento podpůrný materiál slouží jako vodítko k vysvětlení jednotlivých požadavků 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 „vyhláška o kybernetické bezpečnosti“) kladených na smlouvy s dodavateli. Jedná se o vysvětlení jednotlivých požadavků přílohy č. 7 této vyhlášky.

Požadavky na smluvní ustanovení, které vyhláška o kybernetické bezpečnosti ve své příloze č. 7 vyjmenovává, představují povinnou součást smluv povinných subjektů podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) s významnými dodavateli. Pro obsah smluv s ostatními dodavateli má tato příloha doporučující povahu. I v případě, že je stanovena povinnost zařadit taková ustanovení do smlouvy s významným dodavatelem, lze některé požadavky označit za nerelevantní pro danou smlouvu prostřednictvím prohlášení o aplikovatelnosti.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

1 Výklad požadavků vyhlášky o kybernetické bezpečnosti na smlouvy s významným dodavatelem

Požadavek přílohy č. 7 vyhlášky o kybernetické bezpečnosti	Výklad požadavku
Ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity)	Jedná se o ustanovení smlouvy, které reflektuje, zejména, s jakými informacemi dodavatel nakládá a jakým způsobem tak má činit z pohledu důvěrnosti, dostupnosti a integrity (např. pro provozní údaje tzv. logy je klíčová integrita; pro osobní údaje či obchodní tajemství je klíčová zejména důvěrnost apod.). Minimální úrovní splnění tohoto požadavku je ustanovení o uložení těchto dat v souladu s účelem smlouvy a o technických a organizačních opatřeních s tím spojených. Toto ujednání může být obsaženo v samostatné smlouvě tzv. non-disclosure agreement (NDA).
Ustanovení o oprávnění užívat data	Jde o ustanovení smlouvy o právech k datům. Zejména je potřeba stanovit, komu data náleží, kdo k nim má primárně užívací právo. Dále by pak takové ustanovení mělo obsahovat, jakým způsobem má dodavatel s daty nakládat, jak k nim řídit přístup apod. Je vhodné upravit, jak bude s daty a provozními údaji naloženo po ukončení spolupráce, zejména zda a v jaké podobě dojde k předání dat povinnému subjektu nebo zda budou zlikvidována, což připadá v úvahu zejména právě u provozních údajů.
Ustanovení o autorství programového kódu, popřípadě o programových licencích	Jedná se o ustanovení smlouvy upravující zejména, kdo je autorem programového kódu, jakou licencí je kód poskytnut (výhradní/nevýhradní), jaké jsou podmínky užívání programového kódu dle této licence (jak může subjekt s kódem nakládat, např. zda má právo provádět v kódu změny či jej poskytnout třetí osobě, jak bude s programovým kódem naloženo po ukončení spolupráce apod.). Dále se jedná i o ustanovení upravující úpravu a nakládání s dokumentací ke zdrojovému kódu.

Ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu)	Jedná se o ustanovení smlouvy stanovující pravidla pro provádění zákaznického auditu. Zejména jde o samotnou možnost provést zákaznický audit. Dále by obsahem tohoto ustanovení mělo být jak často, jakým způsobem a za jakých podmínek (přítomnost některých osob, ohlášení auditu apod.) lze audit provést. Dále pak rozsah auditu, kam budou mít auditoři přístup apod. Audit může být proveden také třetí stranou a tento audit může být doložen např. auditní zprávou či jiným dokumentem.
Ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele	Jedná se o ustanovení smlouvy zabezpečující promítnutí požadavků na dodavatele i směrem k subdodavatelům. Jde zejména o ujednání, že subdodavatel je povinen dodržovat stejná smluvní ujednání, jaká má sjednána povinný subjekt s dodavatelem.
Ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou	Jedná se o ustanovení smlouvy, které zabezpečuje dodržování bezpečnostních politik povinného subjektu ze strany dodavatele. Toto ustanovení může být (a obvykle tomu tak bude) obsaženo ve všeobecných obchodních podmínkách či jsou tyto politiky přikládány ke smlouvě ve formě jejích příloh.
Ustanovení o řízení změn	Jde o ustanovení smlouvy, které reflektuje způsob, jakým dochází k řízení změn, a to ve dvou rovinách: a) Jakým způsobem probíhá vzájemné schvalování změn obsahu smlouvy. b) Tzv. change management – tedy stanovení přezkumu možných dopadů změn (např. prostřednictvím analýzy rizik), akceptačního procesu (jakým způsobem je změna přijata), testování před nasazením do provozu, promítnutí do bezpečnostních politik, dokumentování změny, možnost navrácení do původního stavu apod. Blíže se této problematice věnuje také § 11 vyhlášky o kybernetické bezpečnosti.

Ustanovení o souladu smluv s obecně závaznými právními předpisy	Jedná se o ustanovení smlouvy obsahující ujednání, že smlouva je v souladu s aktuálními právními předpisy a směřuje k tomu, že smlouva musí plnit aktuální legislativní požadavky a v případě významných legislativních změn musí být upraven způsob, jakým bude těmto požadavkům přizpůsobena.
Ustanovení o povinnosti dodavatele informovat povinnou osobu o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy	Jde o ustanovení smlouvy upravující, že v případě bezpečnostního incidentu souvisejícího s plněním smlouvy u dodavatele se o něm povinný subjekt doví. Zejména je třeba stanovit povinnost dodavatele informovat povinný subjekt o výskytu incidentu (např. jakým způsobem a v jaké lhůtě povinný subjekt dodavatel informuje).
Ustanovení o povinnosti dodavatele informovat povinnou osobu o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy	Jedná se o ustanovení smlouvy, které zavazuje dodavatele, aby povinnému subjektu podal informaci o tom, jakým způsobem řídí rizika a o tom, jaká jsou zbytková rizika související s plněním smlouvy. (např. riziko = špatná konfigurace, opatření = před ostrým provozem otestování, zbytkové riziko = jaké riziko zbyde po nasazení opatření). Je třeba počítat s tím, že i po nasazení bezpečnostního opatření riziko není nulové a vždy tu zbytkové riziko bude.
Ustanovení o povinnosti dodavatele informovat povinnou osobu o významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem	Jde o ustanovení smlouvy o tom, že je třeba povinný subjekt informovat o významné změně ovládání dodavatele. Ovládáním se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení.
Ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy	Jedná se o ustanovení smlouvy navazující na povinnost zmíněnou výše, které zabezpečuje, aby se povinný subjekt o změně kontroly nad dodavatelem dověděl a mohl následně reagovat. Obsahem tohoto ujednání je pak možnost odstoupit od smlouvy v případě, že dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení.

Specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně)	Jde o ustanovení smlouvy, kterým je stanoven postup při ukončení spolupráce s dodavatelem. Jde zejména o stanovení délky přechodného období při ukončení spolupráce (dostatečně dlouhé období, po které má dodavatel povinnost provozovat systém i po ukončení spolupráce), pravidel migrace dat (v jakém formátu a do kdy data a provozní údaje předat povinnému subjektu či novému dodavateli nebo provést jejich likvidaci atd.), poskytování součinnosti budoucímu dodavateli (její rozsah a podmínky), poskytování know-how nasazených řešení budoucímu dodavateli apod. Je třeba myslet i na předání dokumentace spojené s provozem systému.
Specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností)	Jedná se o ustanovení smlouvy upravující zapojení dodavatele do řízení kontinuity činností a specifikace povinností, které má v takovém případě nad rámec běžných povinností. Jedná se také o úpravu změny režimu jeho fungování vůči objednateli, například o zahrnutí (a jeho způsob) dodavatele do plánů kontinuity či do havarijních plánů povinné osoby.
Specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem	Jde o ustanovení smlouvy, kterým je ujednán formát předávaných dat a provozních údajů tak, aby byly pro povinný subjekt použitelná. Data v nesystematizované podobě či strojově nečitelném formátu jsou často pro povinný subjekt či nového dodavatele neupotřebitelná.
Pravidla pro likvidaci dat	Jedná se o ustanovení smlouvy reflektující postup a způsob likvidace dat a provozních údajů. Způsob likvidace dat by měl být stanoven v návaznosti na jejich citlivost a důležitost, někdy postačí pouhé smazání, někdy naopak bude potřeba protokolárně zničit i hmotný nosič, na kterém jsou data zachycena.
Ustanovení o sankcích za porušení povinností	Jde o ustanovení smlouvy, která stanovují sankce za porušení smluvních povinností. Sankce by měly být úměrné k ceně poskytované služby i dopadu případného porušení, aby jejich význam nebyl marginální.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
5. 10. 2018	1.0	Odb. RAP	Vytvoření dokumentu
28. 1. 2019	1.1	Odb. regulace	Změna kontaktních údajů