NÚKIB

POŽADAVKY NA SMLOUVY S DODAVATELI

Verze 1.2, platná ke dni 29. 1. 2021

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. Stejně tak je vhodné ve fázi výběru dodavatele, resp. před uzavřením smlouvy s ním, promítnout obsah jednotlivých požadavků i do procesu hodnocení rizik spojených s předmětem plnění a jeho dodavatelem.

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.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

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 (obvykle půjde o souhrn většího množství ujednání), která reflektují, zejména, s jakými informacemi dodavatel nakládá a jakým způsobem tak má činit z pohledu důvěrnosti, dostupnosti a integrity. V zájmu zajištění jednoznačnosti a přehlednosti práv a povinností smluvních stran je doporučeno do smlouvy či do jejích příloh (příp. navazujících dokumentů) včlenit hodnocení konkrétních informačních aktiv, která jsou předmětem smlouvy, resp. předmětem ochrany z hlediska bezpečnosti informací. Standardně jsou součástí smlouvy též ujednání o povinnosti dodavatele seznámit se se směrnicemi, politikami a metodikami objednatele upravujícími např. pravidla pro manipulaci s informacemi, ochranu informací, likvidaci dat apod., a tato pravidla jsou obvykle odstupňována právě podle klasifikace informačních aktiv. Pokud dodavatel klasifikaci konkrétních aktiv v provozovaném systému nezná, nemůže ani správně aplikovat bezpečnostní opatření uvedená v politikách.

	V rámci smluvního vztahu je třeba explicitně upravit nejen pravidla pro zajištění **důvěrnosti** informací (obvykle formou tzv. non-disclosure agreement, NDA, kde budou obsažena zejm. pravidla o uložení dat, technickém způsobu jejich ochrany, způsobu nakládání s nimi, jejich šíření apod.), ale též pravidla pro zajištění **dostupnosti** informací (obvykle formou tzv. service level agreement, SLA, kde lze definovat např. doby reakce, dobu nastoupení na zásah, dobu opravy poruchy, vyjádření dostupnosti systému v procentech apod.) a **integrity** informací (zde lze uvažovat o požadavcích na šifrování dat, použití elektronického podpisu, aby bylo možné jednoznačně určit, kdo úpravu dat provedl, omezení práv zápisu a úpravy dat na vybrané osoby, řízení přístupu k datům apod.). Zejména ochrana integrity informací a dat je bohužel v mnoha smluvních vztazích opomíjena. Konkrétní podoba smluvních ujednání na ochranu informací bude odvislá i od výsledků procesu hodnocení rizik a přijetí adekvátních bezpečnostních opatření. Dále lze doporučit v rámci těchto ustanovení vyřešit také určení způsobu a výše úhrady účelně vynaložených nákladů na zavedení bezpečnostních opatření, pokud již není jejich úhrada součástí ceny za plnění předmětu smlouvy.
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. Náležitosti související v předáním dat v případě ukončení smluvního vztahu jsou podrobněji rozebrány níže v samostatném bodu.
Ustanovení o autorství programového kódu, popřípadě o programových licencích	Jedná se o ustanovení smlouvy upravující zejména, kdo je autorem zdrojového kódu, na základě jaké licence je program poskytnut (výhradní/nevýhradní), jaké jsou podmínky užívání programu dle této licence (jak může subjekt s programem a kódem nakládat, např. zda má právo provádět v kódu změny či jej poskytnout třetí osobě, jak bude se zdrojovým kódem naloženo po ukončení spolupráce apod.). Dále se jedná i o ustanovení upravující úpravu a nakládání s dokumentací ke zdrojovému kódu. Konkrétním příkladem může být ošetření použití programových komponent třetích stran, např. open source komponent poskytovaných na základě veřejných licencí, popřípadě standardních komerčních řešení třetích stran, ke kterým dodavatel nevykonává majetková autorská práva.
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 také může být proveden třetí stranou a doložen např. auditní zprávou či jiným dokumentem.

	Předmětem auditu by mělo být plnění všech relevantních povinností, ke kterým se dodavatel smluvně zavázal. Typicky půjde o kontrolu způsobu plnění dohodnutých bezpečnostních opatření, způsobu řízení dodavatelů, způsobu nakládání s daty, způsobu identifikace a hlášení kybernetických bezpečnostních incidentů apod. V návaznosti na to je vhodné upravit i řešení zjištěných nedostatků, tedy aby se výsledky auditu reálně projevily v následném plnění smlouvy.
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. Standardně pak platí, že za plnění subdodavatelů odpovídá vůči objednateli sám dodavatel. Výběr subdodavatelů může objednatel každopádně ovlivnit či zcela řídit, ať už schvalováním jednotlivých subdodavatelů či *ex ante* ujednáním kritérií pro jejich výběr.

	V praxi se samozřejmě mohou vyskytnout i situace, kdy dodavatel není schopen zcela ovlivnit podmínky, za jakých jeho poddodavatel vykonává svou činnost (typicky v případech přeprodávání služeb nadnárodních korporací nebo v případech, kde je poddodavatelem mateřská společnost či jiná společnost z koncernu, která dodavateli jakožto své podřízené, obecně slabší entitě určuje, za jakých podmínek bude své služby poskytovat). Povinná osoba tak má na výběr buďto odmítnout podpis smlouvy, neboť dodavatel není schopen dostát jejím požadavkům, nebo přijmout stanovené obchodní podmínky dodavatele za současného přijetí jiného způsobu řízení rizik ve vztahu k poddodavatelům dodavatele (povinnost poddodavatelů řídit se ujednáními povinné osoby a dodavatele tak bude nahrazena např. dalšími bezpečnostními opatřeními mezi povinnou osobou a 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 obsaženo ve všeobecných obchodních podmínkách či jsou tyto politiky přikládány přímo ke smlouvě ve formě jejích příloh.

	Není potřeba seznamovat všechny dodavatele s kompletním obsahem bezpečnostních politik (ty mnohdy obsahují informace směřující výlučně dovnitř organizace, např. obecná pravidla řízení dodavatelů v organizaci, požadavky na bezpečnostní role apod.). Rozsah bezpečnostních politik předložených dodavateli k seznámení se bude odvíjet od specifik smluvního vztahu s tímto dodavatelem, zejm. co je jeho předmětem, jaké plnění bude dodavatel dodávat, plnění jakých bezpečnostních opatření bude dodavatel zajišťovat apod. Typicky, nikoli však výlučně, půjde o ty části bezpečnostních politik, které se věnují zavedení systému řízení bezpečnosti informací (ISMS), zajištění fyzické bezpečnosti v prostorách povinné osoby (pokud do nich bude dodavatel vstupovat), zajištění bezpečnosti vzdáleného přístupu do prostředí povinné osoby (pokud bude využíváno), způsob nakládání s informacemi a jejich klasifikace (pokud bude mít dodavatel k datům přístup) apod. Dodavatel musí být ve výsledku srozuměn se všemi politikami, které by se mohly dotýkat plnění, které povinné osobě poskytuje.
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, podle kterého je povinná osoba povinna přezkoumávat možné dopady změn a určovat a řídit významné změny. Při koncipování smlouvy je tak nezbytné vycházet i z interních politik povinné osoby a reflektovat ve smlouvě např. přijatý způsob identifikace významných změn, způsob jejich řízení apod.
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 (především těmi, které se dotýkají plnění smlouvy) 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. Vždy je nezbytné ve smlouvě specifikovat, s kterými konkrétními předpisy má být plnění v souladu, a pokud je to možné, tak i konkrétní ustanovení jednotlivých předpisů. Obecně závaznými právními předpisy jsou zjednodušeně řešeno všechny normativní právní akty, které nejsou určeny pro individuálně stanovený okruh osob, tj. všechny zákony, vyhlášky, nařízení, evropské předpisy, obecně závazné vyhlášky obcí apod., specifikace těch relevantních, k jejichž dodržování se má dodavatel smluvně zavázat a případně reagovat na jejich změnu, je tak nezbytné. Obecné proklamace o povinnosti dodržovat platné právní předpisy bez dalšího určení mohou ve výsledku vést k prohlášení neurčitosti tohoto ustanovení a k jeho praktické nevymahatelnosti.

	Stejně tak pokud nebude specifikováno, na které předpisy, příp. která konkrétní ustanovení předpisů je v tomto případě myšleno (typicky půjde o předpisy upravující technické požadavky na výrobky, ale také o postup pro nakládání s utajovanými informacemi, o požadavky na podobu a výkon spisové služby apod.), těžko bude možné upravit postup pro případ, že by došlo k jejich změně.
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 dozví. Zejména je třeba stanovit povinnost dodavatele informovat povinný subjekt o výskytu incidentu (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. Pouze deklaratorní ustanovení, kde dodavatel bez dalšího prohlásí, že svá rizika řídí, aniž by byl blíže rozveden způsob či metoda takového řízení, nelze považovat za dostatečné. Stejně tak je důrazně doporučeno si ve smlouvě sjednat možnost kontroly způsobu řízení rizik na straně dodavatele v rozsahu, který se dotýká plnění smlouvy.

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 zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení. Notifikační povinnost může být taktéž navázána na změnu skutečného majitele v evidenci skutečných majitelů (§ 118b a násl. zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů). Zásadními aktivy je třeba rozumět taková aktiva (zejm. programové a technické prostředky či informace, které jsou poskytovány, a zaměstnanci, kteří realizují předmět smlouvy), která jsou určitým způsobem zásadní pro realizaci smluvního závazku, kterými proudí informace povinné osoby nebo skrze která je možné proniknout do systémů objednatele, a jejichž vlastník tak může přímo či nepřímo ovlivňovat bezpečnost dotčeného informačního systému (příp. dalších propojených systémů) a informací v něm (resp. v nich) obsažených. Stanovení způsobu určení zásadních aktiv je věcí povinné osoby a bude ovlivněno především prostředím povinné osoby a specifiky každého jednotlivého smluvního vztahu s dodavatelem. Definice zásadních aktiv v konkrétní smlouvě s konkrétním dodavatelem je tedy vysoce žádoucí.

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, která v souhrnu zabezpečují, 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 zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení. Důležité je, aby se objednatel při definování celého smluvního vztahu vyvaroval plné závislosti na dodavateli (zamezil tzv. *vendor lock-in*). V takovém případě by totiž smlouva sice formálně umožňovala odstoupení, nicméně fakticky by smluvní vztah nebylo možné ukončit (k problematice *vendor lock-in* viz další bod).
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, někdy hovoříme o tzv. exit strategii. 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.

	Správné nastavení těchto podmínek velmi úzce souvisí s problematikou *vendor lock-in* (někdy se používá český pojem proprietární uzamčení), tedy se závislostí objednatele na dodavateli, zpravidla bez faktické možnosti migrace, případně s velmi omezenými možnostmi ukončení stávajícího smluvního vztahu a přechodu k jinému dodavateli. V takovém postavení objednatel v podstatě ztrácí možnost ukončení stávajícího smluvní vztahu, a není tedy v ideální pozici, aby po dodavateli mohl vymáhat plnění veškerých bezpečnostních požadavků, například pod hrozbou přechodu k jinému dodavateli.
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 zejm. v rámci tzv. exit strategie (vhodné je však myslet i na období vlastního plnění smlouvy), kterým je ujednán formát předávaných dat a provozních údajů tak, aby byly pro povinný subjekt použitelné (typicky půjde o požadavek na otevřený a strojově čitelný formát dat, kde bude zaručena kompatibilita v případě migrace). Data v nesystematizované podobě či strojově nečitelném formátu jsou pro povinný subjekt či nového dodavatele obvykle neupotřebitelná.

	Další možností je, že budou určitá data v případě ukončení smluvního vztahu zlikvidována, což připadá v úvahu zejména u provozních údajů. Způsob likvidace bude determinován především bezpečnostními politikami povinné osoby a charakterem likvidovaných dat. Toto ujednání bude zpravidla souviset i s postupem povinné osoby a dodavatele podle § 6a zákona o kybernetické bezpečnosti. V zájmu zajištění jednoznačnosti a transparentnosti postupu při vyžádání a předání informací a dat je vhodné v podrobnostech stanovit zejm. rozsah zpracovávaných a uchovávaných informací, rozsah předávaných dat (zde je vhodné myslet i na předcházení případným problémům s autorskými právy k databázi, příp. jinému dílu, vyjasnit, že součástí předávaných dat jsou i vazby mezi daty apod.), způsob jejich předávání co do formátu i technických prostředků k tomu použitých a další požadavky na podobu procesu předání dat. Alternativně lze ve smlouvě stanovit mechanismy pro dodatečné určení pravidel pro předání informací a dat. Pokud nebudou formát předání informací a dat a další podrobnosti jejich předání (příp. mechanismy pro jejich dodatečné určení) ve smlouvě stanoveny, nelze vyloučit, že výsledný dodavatelem aplikovaný způsob předání informací a dat nebude vyhovovat potřebám povinné osoby.
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.

	Blíže k této problematice viz přílohu č. 4 vyhlášky o kybernetické bezpečnosti. Stanovená pravidla pro likvidaci musí být stanovena přiměřeně tak, aby neúměrně nezatížila povinný subjekt, ale aby byly dodrženy v příloze popsané postupy s ohledem na hodnotu aktiv a další aspekty.
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, respektive aby bylo za použití těchto sankcí možné dodavatele donutit k odstranění nedostatků či k plnění veškerých povinností.

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
28. 1. 2021	1.2	Odb. regulace	Doplnění informací