27. 5. 2026

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Jak nastavit smlouvy s dodavateli podle nové právní úpravy kybernetické bezpečnosti?

Kybernetická bezpečnost již není pouze technickým problémem IT oddělení ani izolovanou compliance agendou. Od 1. listopadu 2025 je účinný zákon č. 264/2025 Sb., o kybernetické bezpečnosti („ZoKB“), který do českého právního řádu provádí požadavky směrnice NIS2 a staví kybernetickou bezpečnost jako odpovědnost celé organizace, včetně jejího vrcholného vedení. Nová právní úprava vyžaduje nejen zavedení technických bezpečnostních opatření, ale také nastavení řízení rizik, vnitřních procesů, kontrolních mechanismů a bezpečnosti dodavatelského řetězce. Z praktického pohledu tak kybernetická bezpečnost zasahuje do fungování celé organizace – od vedení přes právní útvary, compliance až po obchodní útvary odpovědné za výběr dodavatelů a smluvní nastavení dodavatelských vztahů.

Tento článek se zaměřuje na tři hlavní okruhy smluvního nastavení dodavatelských vztahů v oblasti kybernetické bezpečnosti. Nejprve popisuje, jak se v oblasti smluvního nastavení dodavatelských vztahů liší předchozí právní úprava od nové. Následně se věnuje tomu, na které dodavatele tento požadavek skutečně dopadá, tedy proč jsou z pohledu zákona klíčové především ty smluvní vztahy, které souvisejí s aktivy spadajícími do stanoveného rozsahu řízení kybernetické bezpečnosti. Nakonec vysvětluje rozdíly mezi režimem nižších a vyšších povinností a důvody, proč je podle nové právní úpravy nezbytné promítnout bezpečnostní požadavky do smluv s relevantními dodavateli.

Nová úprava totiž staví smlouvu s dodavatelem do zcela jiného světla. Smlouva už nemá řešit jen cenu, úroveň služeb nebo odpovědnost za vady, ale i to, jak bude dodavatel plnit bezpečnostní požadavky a jak bude možné jejich plnění smluvně zajistit a vynucovat.

Podle § 13 odst. 5 ZoKB je poskytovatel regulované služby povinen při zavádění nebo provádění bezpečnostních opatření prostřednictvím dodavatele vybrat tohoto dodavatele v souladu s požadavky vyplývajícími z bezpečnostních opatření a současně tyto požadavky promítnout do smluvní dokumentace. Tato povinnost je výslovná a její význam v nové právní úpravě nelze podceňovat.

Současně však neplatí, že by bylo třeba stejným způsobem přepracovat každou dodavatelskou smlouvu v organizaci. Rozhodující je, zda plnění konkrétního dodavatele souvisí s aktivy, systémy, procesy nebo činnostmi, které spadají do stanoveného rozsahu řízení kybernetické bezpečnosti. Právě zde je těžiště celé úvahy. Smluvní ošetření je klíčové především u těch dodavatelů, jejichž plnění má vazbu na tato aktiva, tedy u těch, jejichž selhání nebo narušení může ovlivnit důvěrnost, integritu nebo dostupnost regulované služby.

Co se oproti předchozí právní úpravě změnilo

Z pohledu dodavatelských smluv je rozdíl mezi předchozí a novou úpravou zásadní.

Předchozí právní rámec zákona č. 181/2014 Sb., o kybernetické bezpečnosti, sice také pracoval s bezpečnostními opatřeními a v určitých případech se promítal i do smluvních vztahů, avšak nová právní úprava jde podstatně dál. Výrazně více akcentuje řízení dodavatelských vztahů jako samostatnou a systémovou součást kybernetické bezpečnosti. Současně výslovně spojuje výběr

dodavatele a obsah smluvní dokumentace s požadavky vyplývajícími z bezpečnostních opatření.

Starší úprava byla v praxi často vnímána tak, že těžiště povinností leží především uvnitř organizace, tedy v interních bezpečnostních opatřeních, dokumentaci a technickém či organizačním nastavení. Nová úprava naproti tomu zřetelně ukazuje, že bez odpovídajícího smluvního nastavení vůči relevantním dodavatelům nelze kybernetickou bezpečnost zajistit v plném rozsahu. Jinými slovy, to, co dříve bylo v mnoha případech spíše doporučeným nebo dovozovaným standardem dobré praxe, se nyní stává mnohem výslovnější regulatorní povinností.

Nová právní úprava je zároveň detailnější i v tom, že rozlišuje intenzitu smluvních požadavků podle režimu povinností a v rámci vyššího režimu navíc pracuje s kategorií významného dodavatele. Tím se smluvní rovina stává jedním z klíčových nástrojů praktické implementace kybernetických povinností.

Rozhodující je vazba na aktiva ve stanoveném rozsahu

Aby bylo možné určit, na které dodavatelské vztahy dopadá povinnost promítnout bezpečnostní požadavky do smluv, je nejprve nezbytné vymezit stanovený rozsah řízení kybernetické bezpečnosti podle § 12 ZoKB. Je tedy třeba určit, která aktiva, systémy, procesy a činnosti skutečně souvisejí s poskytováním regulované služby. Dokud navíc nejsou některá primární nebo podpůrná aktiva řádně posouzena, nahlíží se na ně pro účely zákona tak, jako by do stanoveného rozsahu spadala.

Právě z toho plyne prakticky velmi důležitý závěr. Povinnost smluvního ošetření se nevztahuje automaticky na všechny smlouvy, které poskytovatel regulované služby uzavírá. Rozhodující není název smlouvy ani její formální zařazení, ale skutečný dopad plnění dodavatele na bezpečnost regulované služby. Nedává smysl stejným způsobem upravovat smlouvu na úklid kanceláří, catering a smlouvu na správu klíčové cloudové infrastruktury. Relevantní jsou pouze ty vztahy, u nichž je plnění dodavatele v přímé nebo funkční souvislosti s aktivy ve stanoveném rozsahu.

Tento akcent je zásadní. Smluvní požadavky podle ZoKB se nemají mechanicky přenášet na všechny dodavatele, ale právě na ty, kteří souvisejí s aktivy relevantními pro regulovanou službu. Čím užší a významnější je tato vazba, tím větší důraz musí organizace klást na obsah a vymahatelnost smluvních ujednání.

Samotné právní posouzení nestačí

Vymezení relevantních dodavatelů nemůže být provedeno izolovaně jen jako právní cvičení. Musí navazovat na evidenci aktiv, jejich klasifikaci, řízení rizik a související bezpečnostní dokumentaci. Smluvní úprava je až finálním krokem tohoto procesu. Pokud organizace nemá správně určeno, co spadá do stanoveného rozsahu, nemůže ani přiměřeně a obhajitelně nastavit smluvní požadavky vůči dodavatelům.

V řadě případů navíc nepůjde o zcela zjevné situace. Vedle jednoznačně klíčových dodavatelů, jako jsou poskytovatelé cloudových služeb, provozovatelé infrastruktury nebo vývojáři kritického softwaru, budou existovat i hraniční vztahy, které bude nutné posoudit materiálně, tedy podle konkrétního dopadu na bezpečnost regulované služby.

Režim nižších povinností: základní smluvní standard

U poskytovatelů regulované služby v režimu nižších povinností stanoví vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen „**Vyhláška pro nižší režim**“), v příloze č. 2 okruhy smluvních ujednání, která mají být zohledněna

ve smlouvách s dodavateli, jejichž plnění spadá do stanoveného rozsahu řízení kybernetické bezpečnosti. Vyhláška současně výslovně ukládá povinnost uzavírat pouze takové smlouvy, které stanoví způsob realizace bezpečnostních opatření a vymezují odpovědnost smluvních stran za jejich zavedení a kontrolu.

Příloha č. 2 představuje základní rámec smluvního ošetření relevantních dodavatelských vztahů. Zahrnuje zejména oblasti bezpečnosti informací, auditu dodavatele, zapojení poddodavatelů, ukončení smluvního vztahu z pohledu ochrany informací, sankčních mechanismů, oprávnění k užití dat, autorství programového kódu, důvěrnosti, bezpečnostních politik, řízení změn, řešení kybernetických bezpečnostních incidentů, zajištění kontinuity činností, úrovně poskytovaných služeb a pravidel bezpečného vývoje.

Ani v režimu nižších povinností tedy nepostačuje obecná deklarace dodavatele, že bude dodržovat právní předpisy nebo postupovat bezpečně. Taková ujednání bývají v praxi málo použitelná a obtížně vymahatelná, zejména při incidentu. Pokud ve smlouvě chybí konkrétní mechanismy, například auditní oprávnění, oznamovací povinnosti, pravidla pro zapojení poddodavatelů nebo podmínky předání a ochrany dat, dostává se poskytovatel regulované služby do situace, kdy sice formálně deklaruje soulad, ale fakticky postrádá nástroje, jak bezpečnostní požadavky vůči dodavateli prosadit.

Současně je třeba dodat, že příloha č. 2 nepředstavuje mechanický seznam, který musí být bez dalšího převzat do každé smlouvy. Rozsah konkrétních ujednání musí odpovídat povaze plnění, jeho významu pro regulovanou službu a míře zapojení dodavatele do stanoveného rozsahu. U jednodušší podpůrné služby bude smluvní rámec užší než u dodavatele, který spravuje produkční prostředí nebo vyvíjí kritický software. Každá odchylka od doporučeného standardu však musí být racionálně odůvodněna a přiměřeně zdokumentována.

Režim vyšších povinností: přísnější a systematičtější přístup

U poskytovatelů regulované služby v režimu vyšších povinností je přístup k řízení dodavatelů systematičtější a současně přísnější. ZoKB v § 14 mezi organizačními opatřeními výslovně počítá s řízením dodavatelských vztahů a vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „**Vyhláška pro vyšší režim**“), tento rámec dále rozpracovává.

Klíčovým rozdílem oproti nižšímu režimu je potřeba rozlišovat mezi běžnými relevantními dodavateli a významnými dodavateli. Právě u významných dodavatelů se uplatní zesílený smluvní standard vycházející z přílohy č. 5 Vyhlášky pro vyšší režim.

Za významného dodavatele se považuje dodavatel, jehož plnění má zásadní význam pro zajištění kybernetické bezpečnosti regulované služby. Nejde o formální označení, ale o materiální hodnocení. Typicky sem budou spadat dodavatelé s vysokou úrovní přístupů k systémům, s kontrolou nad klíčovými technologiemi, s přístupem k citlivým datům, s významným vlivem na dostupnost a fungování regulované služby nebo takoví, jejichž rychlá náhrada by byla v krizové situaci obtížná. I zde je tedy rozhodující vazba na aktiva a činnosti ve stanoveném rozsahu, nikoli jen obchodní význam dodavatele jako takového.

Co musí řešit smlouva s významným dodavatelem

Ve vztahu k dodavatelům, kteří významnými dodavateli nejsou, právní úprava nestanoví povinnost mechanicky aplikovat požadavky přílohy č. 5. To však neznamená, že by bylo možné smluvní úpravu

opomenout. I v těchto případech musí smluvní rámec odpovídat tomu, že se dodavatel podílí na zavádění nebo provádění bezpečnostních opatření. V praxi to obvykle znamená alespoň základní balík ustanovení o bezpečnosti informací, řešení incidentů, auditních oprávněních, řízení změn, poddodavatelích, kontinuitě a ukončení smluvního vztahu.

U významných dodavatelů je však požadovaný standard podstatně robustnější. Příloha č. 5 Vyhlášky pro vyšší režim stanoví výrazně širší a detailnější rámec smluvních ujednání. Vedle základních oblastí zahrnuje i další specifické požadavky, například povinnost dodavatele informovat o způsobu řízení rizik a o zbytkových rizicích, o významných změnách v ovládání dodavatele nebo v zásadních aktivech, o změnách týkajících se aktiv využívaných k plnění, o žádostech cizozemských orgánů o zpřístupnění dat nebo o osobách přicházejících do kontaktu s důvěrnými informacemi. Smluvní úprava musí dále řešit pravidla pro předání a likvidaci dat a také právo poskytovatele regulované služby ukončit smluvní vztah bez výpovědní doby v určitých závažných situacích na straně dodavatele.

Právě u těchto smluv se v praxi často ukazuje, že standardní dodavatelská dokumentace na nové požadavky nestačí. Dodavatelé bývají zdrženliví například vůči širším auditním oprávněním, transparentnějším pravidlům pro poddodavatele, smluvně silnějším právům při ukončení spolupráce nebo vůči informačním povinnostem o změnách na své straně. Právě zde se ale ukazuje rozdíl mezi běžnou obchodní smlouvou a smlouvou, která obstojí i z pohledu kybernetické regulace.

Nejčastější slabá místa v praxi

Z praxe lze identifikovat několik opakujících se nedostatků.

Prvním je oddělené řešení smluvní roviny bez návaznosti na klasifikaci dodavatelů, evidenci aktiv a řízení rizik. Druhým je spoléhání na obecná ustanovení o mlčenlivosti nebo úrovni služeb, která specifické požadavky kybernetické bezpečnosti nepokrývají dostatečně. Třetím častým problémem je nedostatečné ošetření poddodavatelského řetězce, kdy smluvní povinnosti nejsou efektivně přenášeny na další zapojené subjekty. Slabým místem bývá také absence funkční strategie ukončení spolupráce, která by zajistila kontrolu nad daty a kontinuitu služeb po skončení smluvního vztahu.

Podceňována bývá i dokumentace. Nejen samotné smlouvy, ale i úvahy, proč byl konkrétní dodavatel považován za relevantního či významného a proč byla určitá smluvní ujednání použita nebo naopak nepoužita, by měly být dohledatelné a obhajitelné.

Sankce nejsou pouze teoretické

Podcenit smluvní rovinu se nevyplácí. Zákon výslovně řadí mezi přestupky i situaci, kdy poskytovatel regulované služby nevybírá dodavatele v souladu s požadavky vyplývajícími z bezpečnostních opatření nebo tyto požadavky nezahrne do smlouvy v rozporu s § 13 odst. 5 ZoKB. To platí jak pro režim vyšších povinností, tak pro režim nižších povinností.

Sankční expozice je přitom významná. V režimu vyšších povinností může pokuta dosáhnout až 250 milionů Kč nebo 2 % čistého celosvětového ročního obratu, v režimu nižších povinností pak až 175 milionů Kč nebo 1,4 % obratu, podle toho, která částka je vyšší. Vedle finančních sankcí může NÚKIB uložit i nápravná opatření, která mohou mít v praxi citelný dopad na provoz poskytovatele regulované služby.

Jak k tomu přistoupit systematicky

Implementace smluvních požadavků by měla probíhat postupně a systematicky. Základem je identifikace a kategorizace dodavatelů podle jejich vztahu k aktivům a činnostem ve stanoveném rozsahu řízení kybernetické bezpečnosti a podle míry rizika.

Na tento krok navazuje cílená revize stávajících smluv, přičemž prioritu by měly mít vztahy s významnými a jinak rizikovými dodavateli. Současně je vhodné vytvořit standardizované smluvní moduly, tedy základní bezpečnostní přílohu pro relevantní dodavatele, rozšířený modul pro rizikovější vztahy a zesílený standard pro významné dodavatele.

Smluvní rámec však bude fungovat pouze tehdy, pokud bude provázán s interními procesy a bezpečnostní dokumentací. Ustanovení o auditu nedává smysl, pokud organizace neví, kdo audit provede. Ujednání o oznamování bezpečnostních incidentů nebude prakticky použitelné, pokud není jasné, komu se incident hlásí a jaký je postup jeho eskalace. Povinnost dodržovat bezpečnostní politiky zůstane slabá, pokud tyto politiky nejsou aktuální, použitelné a skutečně zavedené do praxe.

Shrnutí

Nová právní úprava kybernetické bezpečnosti v České republice zásadně mění přístup k dodavatelským smlouvám. Smluvní vztahy již nepředstavují pouze nástroj pro vymezení obchodních podmínek, ale stávají se klíčovým prostředkem pro zajištění a prosazení bezpečnostních požadavků.

Klíčové přitom je, že tento důraz se netýká všech dodavatelů bez rozdílu, ale především těch, jejichž plnění souvisí s aktivy a činnostmi spadajícími do stanoveného rozsahu řízení kybernetické bezpečnosti. Právě u těchto dodavatelů musí být organizace schopna prokázat, že bezpečnostní požadavky promítla do smluvní dokumentace přiměřeně významu a rizikovosti jejich plnění.

V režimu nižších povinností jde o základní, avšak poměrně široký smluvní standard. V režimu vyšších povinností je pak nezbytné navíc rozlišovat významné dodavatele, u nichž právní úprava vyžaduje podstatně robustnější a detailnější smluvní rámec. Nedostatečné smluvní ošetření přitom nepředstavuje pouze otázku kvality kontraktace, ale i významné regulatorní riziko.

Ve zkratce: jednou z největších chyb je domnívat se, že kyberbezpečnostní soulad lze zajistit jen interní politikou. Nelze. Bez dobře nastavených smluv s těmi dodavateli, kteří souvisejí s relevantními aktivy a podílejí se na bezpečnosti regulované služby, zůstane velká část povinností jen na papíře.

Mgr. Bc. Laura Mesarošová

Weinhold Legal

Weinhold Legal, s.r.o. advokátní kancelář

Florentinum
Na Florenci 2116/15
110 00 Praha 1

Tel.: +420 225 385 333
Fax: +420 225 385 444

e-mail: wl@weinholdlegal.com

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus