PORTÁL NÚKIB

Zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti

TLP:CLEAR

9. červen 2026

Verze 1.0

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

Předmluva – jak metodiku používat

Účelem tohoto dokumentu je poskytnout zadavatelům veřejných zakázek, kteří pořizují informační a komunikační technologie a s nimi spojené služby, podporu při zadávání veřejných zakázek tak, aby postupovali v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“), a současně naplnili povinnosti vyplývající z právní úpravy kybernetické bezpečnosti, tedy zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZKB“). Dokument se zaměřuje na situace, kdy může formalizovaný proces zadávání veřejných zakázek dopadat na potřebu efektivně zajišťovat odpovídající úrovně kybernetické a informační bezpečnosti, a shrnuje možnosti, které mají zadavatelé k dispozici.

Metodika vychází z nové právní úpravy kybernetické bezpečnosti, zejména ze ZKB a z jeho prováděcích právních předpisů, tj. vyhláška č. 408/2025 Sb., o regulovaných službách, vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností a další. Původní právní rámec obsažený v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „starý ZKB“) byl nahrazen. Varování a další akty vydané podle starého ZKB však zůstávají v účinnosti a podle přechodných ustanovení se považují za akty vydané podle ZKB.

Dokument je určen zejména zadavatelům, kteří jsou současně poskytovateli regulovaných služeb podle ZKB, ať již v režimu vyšších nebo nižších povinností. Rozsah a podrobnosti povinností jednotlivých kategorií povinných osob nejsou v této metodice podrobně rozpracovány. Pro účely sebeidentifikace, ohlášení regulované služby, stanovení rozsahu řízení kybernetické bezpečnosti jako základní hrací plochy a orientace v režimech regulace se odkazuje na informační materiály dostupné na Portálu NÚKIB (zejména „Průvodce novým zákonem o kybernetické bezpečnosti“ a související podpůrné materiály).

Metodika může být užitečná i pro zadavatele, na něž se ZKB formálně nevztahuje. V těchto případech může sloužit jako vodítko pro přiměřené nastavení požadavků na kybernetickou a informační bezpečnost v zadávacích řízeních, zejména tam, kde zadavatel zajišťuje veřejné služby nebo služby významné pro fungování veřejné správy. Zohledňování bezpečnostních opatření totiž bude často představovat legitimní zájem také v organizacích, na které nedopadá osobní působnost ZKB, resp. které se neidentifikují jako poskytovatelé regulovaných služeb, a přesto své služby chtějí řádně zabezpečit.

Metodika není komplexním návodem pro postup zadavatele podle ZZVZ ani úplným výkladem ZKB. Zaměřuje se především na průnik obou oblastí – tj. na to, jak výsledky procesu řízení rizik a dalších bezpečnostních opatření podle ZKB promítnout do přípravy, průběhu a plnění veřejných zakázek v oblasti ICT a kybernetické bezpečnosti.

Metodiku je vhodné používat tak, že zadavatel:

- vychází z vlastního procesu řízení rizik a bezpečnostní dokumentace podle ZKB a prováděcích právních předpisů,
- identifikuje problematické oblasti, v nichž se střetávají požadavky ZZVZ a ZKB (např. omezení rizikových technologií, práce s dodavatelským řetězcem, ochrana důvěrných informací),
- využije jednotlivé kapitoly metodiky jako podpůrné vodítko pro volbu zadávacích podmínek, výběr vhodného zadávacího postupu a nastavení nebo úpravu smluvních ujednání.

Metodika vznikla ve spolupráci následujících organizací:

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)
Mučednická 1125/31
616 00 Brno

Asociace pro veřejné zakázky, z.s.
Husitská 344/63
130 00 Praha

Úřad pro ochranu hospodářské soutěže (ÚOHS)
třída Kpt. Jaroše 7
602 00 Brno

Upozornění:

Metodika slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu je vyhrazeno. Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti zveřejněné verze dokumentu.

Pro účely zjednodušení metodika vychází především z pravidel, která se typicky uplatní u veřejných zakázek zadávaných v zadávacím řízení v nadlimitním režimu podle ZZVZ. V řadě případů jsou zde popsané postupy a principy použitelné i pro jiné režimy zadávání veřejných zakázek (např. podlimitní režim nebo veřejné zakázky malého rozsahu).

Zadavatel by však měl vždy posoudit, zda jsou jednotlivé závěry a doporučení přiměřené konkrétnímu postupu a režimu, v němž veřejnou zakázku zadává, a přizpůsobit jejich aplikaci konkrétním okolnostem.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

1 Rámec a východiska

Tato kapitola vymezuje základní pojmy, role a právní rámec, ze kterého metodika vychází. Cílem je sladit pohled zadavatelů, kteří zadávají veřejné zakázky v oblasti ICT a kybernetické bezpečnosti, s požadavky ZKB a vytvořit tak společný výchozí bod pro další, praktičtěji zaměřené části metodiky.

Vedle ZZVZ a ZKB mají na problematiku zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti vliv ještě následující oblasti a předpisy, bezprostředně související s touto problematikou, ve znění pozdějších předpisů (jsou-li novelizovány). Uvedený výčet není vyčerpávající a nezahrnuje všechny právní předpisy, které mohou na konkrétní veřejnou zakázku dopadat v závislosti na jejím předmětu, odvětví nebo specifických okolnostech:

- Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 (tzv. AI Act),
- 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 (tzv. Nařízení GDPR),
- Nařízení č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (tzv. Nařízení eIDAS),
- Nařízení Evropského parlamentu a Rady (EU) 2024/1183, kterým se mění nařízení (EU) č. 910/2014 (eIDAS) (tzv. Nařízení eIDAS 2.0),
- Zákon č. 110/2019 Sb., o zpracování osobních údajů,
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
- Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

1.1 Terminologie a role zadavatele

Pro účely této metodiky se používají zejména následující pojmy ve významu vymezeném právní úpravou kybernetické bezpečnosti:

- **Regulovaná služba** – služba splňující podmínky pro registraci regulované služby vymezené v § 4 či § 5 ZKB, o které NÚKIB rozhodl podle § 6 odst. 2 ZKB. Seznam služeb a vymezení podmínek významnosti poskytovatele stanovuje vyhláška č. 408/2025 Sb., o regulovaných službách.
- **Aktiva** – fyzické nebo digitální prostředky, osoby nebo činnosti související se zpracováváním informací a dat v elektronické podobě.

- **Primární aktiva** – aktiva v podobě zpracovávaných informací nebo poskytovaných služeb.
- **Podpůrná aktiva** – aktiva zajišťující fungování primárních aktiv, zejména zaměstnanci, dodavatelé, technická aktiva, budovy a jiné ohraničené prostory, ve kterých se nachází aktivum regulované služby.
- **Technická aktiva** – technický nebo programový prostředek anebo vybavení (jde o druh podpůrného aktiva).
- **Bezpečnostní opatření** – technická a organizační opatření podle § 13 a § 14 ZKB, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.
- **Významný dodavatel** – ten, kdo povinné osobě poskytuje plnění, které je významné z hlediska zajištění kybernetické bezpečnosti regulované služby.
- **Varování** – protiopatření vydané NÚKIB podle § 22 ZKB, kterým je upozorněno na závažnou hrozbu nebo zranitelnost v oblasti kybernetické bezpečnosti.
- **Analýza rizik** – proces identifikace, hodnocení a vyhodnocení rizik ve vztahu k chráněným aktivům, jehož výsledkem je rozhodnutí o akceptovatelnosti rizik a o volbě přiměřených bezpečnostních opatření.
- **Service Level Agreement (SLA)** – dohoda o úrovni poskytovaných služeb, smlouva mezi poskytovatelem služeb (ICT, kybernetická bezpečnost, hosting) a objednatelem. Definuje parametry kvality služby, jako je dostupnost, rychlost reakce při výpadku a případně sankce za jejich nedodržení.

Tyto pojmy jsou v metodice používány v návaznosti na právní úpravu ZKB a jeho prováděcích právních předpisů a je třeba je vykládat konzistentně v celém dokumentu.

1.1.1 Role zadavatele v kontextu ZKB

Zadavatel veřejné zakázky v oblasti ICT a kybernetické bezpečnosti může vystupovat v různých rolích z pohledu právní úpravy kybernetické bezpečnosti. V řadě případů je zadavatel současně poskytovatelem regulované služby podle ZKB, a to buď v režimu vyšších, nebo nižších povinností. To má přímý dopad na rozsah a intenzitu bezpečnostních opatření, která je zadavatel povinen zavádět, a tím i na míru, v jaké je třeba problematiku kybernetické bezpečnosti zohledňovat v zadávacích podmínkách jím zadávaných veřejných zakázek.

Poskytovatelé regulovaných služeb v režimu vyšších povinností jsou povinni zavádět komplexní systém řízení kybernetické bezpečnosti, včetně rozšířeného řízení rizik, řízení dodavatelů a bezpečnostních opatření pokrývajících celý životní cyklus informačních a komunikačních systémů. Tomu odpovídá i širší prostor pro uplatnění bezpečnostních požadavků v zadávacích podmínkách (včetně těch smluvních).

U poskytovatelů regulovaných služeb v režimu nižších povinností je nutné rozsah bezpečnostních opatření, a zejména jejich promítnutí do zadávacích podmínek, posuzovat více individuálně a přiměřeně povaze regulované služby a významu dotčených aktiv.

Zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti není v tomto kontextu samostatnou nebo izolovanou činností, ale představuje jeden z nástrojů, jak zadavatel naplňuje své povinnosti v oblasti kybernetické a informační bezpečnosti. Zadavatel tedy nevstupuje do zadávacího řízení „neutrálně“, ale s již existujícím bezpečnostním rámcem, který vyplývá z jeho interní dokumentace, analýzy rizik a přijatých bezpečnostních opatření podle ZKB a jeho prováděcích právních předpisů.

Vedle zadavatelů, kteří jsou povinnými osobami podle ZKB, existují také zadavatelé, na něž se osobní působnost ZKB formálně nevztahuje. I tito zadavatelé však mohou mít legitimní zájem na zajištění odpovídající úrovně kybernetické a informační bezpečnosti, zejména pokud zajišťují veřejné služby nebo provozují informační systémy významné pro veřejnou správu. Pro tyto subjekty může být právní rámec ZKB a s ním spojené postupy řízení rizik a dodavatelů vhodným referenčním základem pro přiměřené nastavení zadávacích podmínek.

Z pohledu lidských zdrojů musí být do přípravy a realizace veřejné zakázky v oblasti ICT a kybernetické bezpečnosti zapojena řada různých rolí. Konkrétní role a rozložení odpovědností se může lišit dle kontextu organizace. Příkladem lze zmínit:

- **vedení zadavatele**: schvaluje rizikovou úroveň, rozpočet, klíčové milníky, rozhoduje o výběru dodavatele, podepisuje smlouvu,
- **garanti aktiv sloužících k poskytování regulované služby**: definují potřeby, spolupracují při analýze rizik, tvorbě zadávací dokumentace a akceptaci,
- **právní oddělení zadavatele/specialisté nákupu**: zajišťuje zákonnost postupu, promítá požadavky do zadávací dokumentace, administruje proces zadávacího/výběrového řízení,
- bezpečnostní garant: formuluje bezpečnostní požadavky,
- **IT architekt/technický garant**: navrhuje architekturu, ověřuje kompatibilitu a testovatelnost; připravuje akceptační testy,
- **projektový manažer**: řídí realizaci investiční akce, zodpovídá za zdárný průběh projektového cyklu,
- **hodnoticí komise**: posuzuje a hodnotí nabídky, měla by zahrnovat osoby, kompetentní ve všech uvedených oblastech,
- **provozní správce** (po uzavření smlouvy a v provozní fázi): přebírá službu, sleduje dodržování SLA, KPI (Key Performance Indicators) a KRI (Key Risk Indicators), vyžaduje nápravu a vede změnové řízení.

Navazujícím lidských zdrojem je pak samotný vybraný dodavatel, resp. jeho zaměstnanci a vedoucí pracovníci, případně i další pracovníci poddodavatelů vybraného dodavatele, kteří v rámci realizační fáze veřejné zakázky přicházejí se zaměstnanci zadavatele do přímého osobního kontaktu. Řádné ustanovení a definování všech uvedených rolí je klíčovým předpokladem úspěšné realizace veřejné zakázky v oblasti ICT a kybernetické bezpečnosti.

1.1.2 Typy veřejných zakázek z pohledu kybernetické bezpečnosti

Z pohledu kybernetické bezpečnosti není každá veřejná zakázka spojena se stejnou mírou rizika ani se stejnými požadavky na bezpečnostní opatření. Charakter a význam poptávaného plnění mají přímý vliv na rozsah analýzy rizik, na intenzitu bezpečnostních opatření a s nimi související míru případného omezení hospodářské soutěže, kterou je možné ze strany zadavatel obhájit. Rozlišení typů veřejných zakázek ve vztahu k primárním a podpůrným aktivům proto představuje důležité východisko pro další práci s riziky a zadávacími podmínkami.

Ve vztahu k primárním a podpůrným aktivům regulované služby lze rozlišit následující typy veřejných zakázek:

a) Veřejné zakázky na pořízení nebo rozvoj podpůrných aktiv, nezbytných pro provoz a funkčnost primárních aktiv (např. vlastní SW pro informační systém, servery, disková úložiště a síťová infrastruktura apod.),
b) Veřejné zakázky na zavedení nebo rozvoj bezpečnostních opatření k ochraně primárních a podpůrných aktiv, zejména technických a organizačních opatření podle ZKB (např. zařízení typu SIEM, firewall, netflow sonda, kryptografické prostředky, kamerový systém serverovny apod.),
c) Veřejné zakázky zahrnující přímé nakládání s primárními aktivy, zejména služby, při nichž dochází k přístupu k datům nebo systémům regulované služby, jejich správě, provozu nebo jiné formě zásahu do jejich funkce (např. záloha či migrace dat primárních aktiv apod.).

Uvedené typy veřejných zakázek představují orientační členění podle povahy vztahu plnění k primárním a podpůrným aktivům regulované služby. V praxi se jednotlivé typy mohou kombinovat, zejména u veřejných zakázek na provoz, správu, outsourcing nebo poskytování ICT služeb formou služeb (např. cloudových služeb nebo modelu SaaS), které současně zahrnují pořízení nebo rozvoj podpůrných aktiv a přímé nakládání s primárními aktivy.

Pro účely posouzení dopadů do kybernetické bezpečnosti je vždy rozhodující skutečný rozsah přístupu dodavatele k primárním a podpůrným aktivům a míra jeho vlivu na poskytování regulované služby, nikoli formální označení typu veřejné zakázky.

Vedle vlastních veřejných zakázek, které se vztahují k regulovaným službám, hrají významnou roli tzv. varování NÚKIB dle § 22 ZKB, která mají bezprostřední dopad do zadávání výše uvedených veřejných zakázek, bez ohledu na to, v jaké fázi se nachází konkrétní zadávací řízení nebo celý životní cyklus předmětné veřejné zakázky. Institut varování NÚKIB je blíže popsán v kapitole 1.3.

1.2 Právní rámec: Vztah ZZVZ a ZKB

Pro vzájemný vztah ZZVZ a ZKB platí, že jsou to právní předpisy stejné právní síly. Nenacházejí se ve vztahu nadřízenosti či podřízenosti a v zásadě nejsou v rozporu. Orgány a osoby, které podléhají oběma zákonům, jsou povinny postupovat tak, aby dostály požadavkům obou předpisů současně.

ZZVZ požaduje, aby zadavatel při postupu podle tohoto zákona dodržoval zásady transparentnosti a přiměřenosti (§ 6 odst. 1 ZZVZ) a ve vztahu k dodavatelům zásadu rovného zacházení a zákazu diskriminace (§ 6 odst. 2 ZZVZ). Na uvedené navazuje požadavek, aby zadávací podmínky nevytvářely bezdůvodné překážky hospodářské soutěže a nezaručovaly některým dodavatelům neopodstatněnou konkurenční výhodu (§ 36 odst. 1 ZZVZ). Teritoriální rámec těchto zásad pak definuje § 6 odst. 3 ZZVZ, který zadavatelům umožňuje tyto zásady selektivně nepoužít vůči tzv. dodavatelům ze třetích zemí. Více o této problematice pojednává kapitola 3 této metodiky.

ZKB naopak vyžaduje, aby povinné osoby zaváděly a prováděly bezpečnostní opatření v míře nezbytné pro zajištění kybernetické bezpečnosti a aby byla tato opatření uplatněna i ve vztahu k dodavatelům. Součástí toho je mj. řízení rizik, řízení dodavatelů a reakce na protiopatření, mezi něž patří i institut varování NÚKIB.

ZKB zároveň představuje transpozici směrnice EU, tzv. směrnice NIS2[1] do českého právního řádu, ostatně jako ZZVZ představuje transpozici zadávací směrnice EU, a navazuje tak na jednotný evropský rámec pro kybernetickou bezpečnost ve vybraných odvětvích. Směrnice NIS2 a v důsledku rovněž ZKB ve srovnání s předchozí právní úpravou (starým ZKB) výrazně rozšířil okruh regulovaných osob a zpřísnily požadavky na řízení rizik a bezpečnostní opatření.

Z pohledu zadavatele veřejných zakázek v oblasti ICT a kybernetické bezpečnosti je klíčové, že:

- bezpečnostní požadavky vyplývající ze ZKB (včetně požadavků přijatých na základě analýzy rizik, varování nebo jiných protiopatření NÚKIB) mohou vést k omezení okruhu přípustných řešení nebo dodavatelů,
- takové omezení hospodářské soutěže, které je transparentně a srozumitelně upraveno v zadávacích podmínkách veřejné zakázky, není samo o sobě nezákonné, pokud je:

    1. objektivně odůvodněno povinnostmi podle ZKB,
    2. přiměřené z hlediska cíle (zajištění požadované úrovně kybernetické bezpečnosti), a
    3. zadavatel má k dispozici vnitřně konzistentní a přezkoumatelné podklady, z nichž vyplývá, proč byly konkrétní bezpečnostní požadavky zvoleny.

Dle soudní judikatury obecně platí, že zadávací podmínky by měly být koncipovány tak, aby byla zaručena spravedlivá soutěž dodavatelů schopných realizovat veřejnou zakázku, ale také aby plnění veřejné zakázky dle zadávacích podmínek bylo způsobilé naplnit potřeby a legitimní očekávání zadavatele. Z povahy věci by nebylo spravedlivé na zadavateli požadovat, aby zadávací podmínky měly vždy na všechny dodavatele stejný dopad. Zadavatel je proto oprávněn stanovit i takové zadávací podmínky, v jejichž důsledku bude vyloučena určitá skupina dodavatelů na trhu z možnosti ucházet se o veřejnou zakázku (rozsudek Krajského soudu v Brně ze dne 30. 09. 2021, sp. zn. 29 Af 53/2019–70).

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS2).

Naplnění povinností podle ZKB nemůže být považováno za neodůvodněné omezení hospodářské soutěže. Naopak je povinností zadavatele vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření a zahrnovat tyto požadavky do smluv s dodavatelem (§ 13 odst. 5 ZKB). To například znamená povinnost promítnout do zadávacích podmínek ta bezpečnostní opatření, která vyplývají z analýzy rizik. Přičemž vstupem do analýzy rizik může být zejména varování či jiná protiopatření NÚKIB, jež se k danému plnění vztahují.

Směrnice NIS2 a ZKB zároveň kladou důraz na odpovědnost vedení organizace a na systematický přístup k řízení rizik. To se promítá i do této metodiky: zadávací řízení nepředstavuje izolovaný proces, ale navazuje na interní řízení rizik a bezpečnostní dokumentaci. Zadavatel by proto zpravidla neměl „nastavovat bezpečnost od nuly“ jen pro účely zadání konkrétní veřejné zakázky, ale vycházet z již existujícího systému řízení bezpečnosti informací uvnitř organizace.

ZKB ani prováděcí právní předpisy nevyžadují, aby zadavatel prováděl samostatnou analýzu rizik ke každé jednotlivé veřejné zakázce. Zadávací řízení má vycházet z existujícího a průběžně aktualizovaného systému řízení rizik organizace. Konkrétní veřejná zakázka se pak posuzuje z hlediska toho, zda spadá do již vyhodnoceného rámce, případně zda vyžaduje cílené doplnění či zpřesnění již existujícího hodnocení rizik.

Institut varování NÚKIB je v tomto rámci specifickým vstupem do řízení rizik i do zadávání veřejných zakázek. Práci s varováním podrobně rozpracovává následující kapitola.

1.3 Institut varování NÚKIB

Institut varování je jedním ze základních nástrojů, který má NÚKIB k dispozici pro ochranu kybernetické a informační bezpečnosti v České republice.

Dle § 20 odst. 1 ZKB se varování řadí mezi tzv. *protiopatření*, vedle *výstrahy* a *reaktivního protiopatření*.

Samotný institut varování je upraven v § 22 ZKB, který stanoví, že NÚKIB vydá varování, dozví-li se o závažné hrozbě nebo zranitelnosti v oblasti ICT a kybernetické bezpečnosti, a že tuto informaci sděluje dotčeným poskytovatelům regulovaných služeb a zpravidla ji zveřejňuje na úřední desce.

1.3.1 Varování v režimu ZKB a návaznost na dřívější varování

ZKB zachovává institut varování jako nástroj, kterým NÚKIB sděluje, že určitý jev (např. konkrétní technologie, architektura, způsob provozu, lokalita zpracování dat nebo dodavatelský model) představuje hrozbu určité intenzity, se kterou musí povinné osoby pracovat v rámci řízení rizik.

Zároveň platí, že varování vydaná podle starého ZKB zůstávají v účinnosti i po nabytí účinnosti ZKB. Přechodné ustanovení § 71 odst. 3 ZKB výslovně stanoví, že varování vydaná podle starého ZKB se považují za varování vydaná podle ZKB.

Ve vztahu k zadavatelům veřejných zakázek jsou ke dni vydání této metodiky relevantní mimo jiné zejména:

- varování NÚKIB ze dne 17. 12. 2018 před použitím technických a programových prostředků společností Huawei a ZTE,
- varování NÚKIB ze dne 3. 9. 2025 před předáváním systémových a uživatelských dat na území ČLR a výkonem vzdálené správy technických aktiv z území ČLR (včetně zvláštních administrativních oblastí).

Všechna varování je tedy nutné vnímat jako součást systému protiopatření podle ZKB, bez ohledu na to, podle jaké právní úpravy byla původně vydána.

1.3.2 Varování jako vstup do řízení rizik

Varování samo o sobě nepředepisuje konkrétní technické nebo organizační opatření a neznamená automatický zákaz určité technologie, řešení či dodavatele v zadávacím řízení. Z pohledu ZKB jde o vstup do řízení rizik:

- § 13 odst. 2 ZKB ukládá poskytovatelům regulovaných služeb povinnost zavádět a provádět bezpečnostní opatření v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby,

- § 14 odst. 1 písm. a) ZKB mezi organizačními bezpečnostními opatřeními pro poskytovatele regulovaných služeb v režimu vyšších povinností výslovně uvádí řízení rizik a řízení dodavatelů, která tvoří rámec pro práci s varováním zadavatelů veřejných zakázek.

Z praktického hlediska to znamená, že:

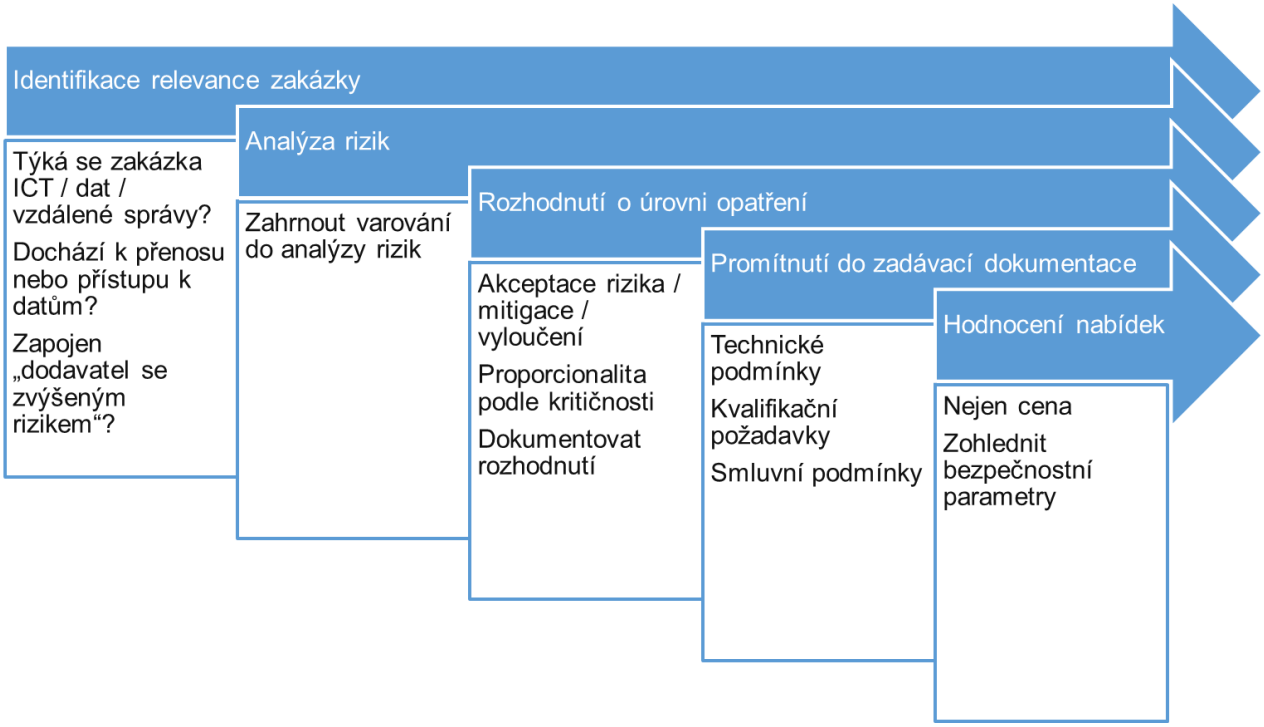
- varování identifikuje existenci závažné hrozby nebo zranitelnosti (§ 22 odst. 1 ZKB),
- poskytovatel regulované služby v režimu vyšších povinností musí tuto hrozbu zařadit do své analýzy rizik v rámci stanoveného rozsahu řízení kybernetické bezpečnosti (§ 12 a § 14 ZKB),
- výsledkem musí být rozhodnutí, zda je riziko spojené s jevem popsaným ve varování akceptovatelné (a tudíž nevyžaduje přijetí žádných opatření), nebo zda je nutné přijmout dodatečná bezpečnostní opatření (např. omezení určitých technologií, dodavatelů, lokalit zpracování dat nebo způsobů vzdálené správy).

Poskytovatelé regulované služby v režimu nižších povinností nemusí provádět přímo dokumentovanou analýzu rizik, tak jako tomu je v režimu vyšších povinností. To však neznamená, že by se poskytovatelé těchto regulovaných služeb měli úvahám nad možnými riziky zcela vyhnout. Stále pro ně platí povinnost zohledňovat své bezpečnostní potřeby a alespoň rámcově uvažovat nad riziky a dopady. Přičemž platí, že zohlednění varování může být pro poskytovatele regulované služby v režimu nižších povinností přeneseně povinné, jestliže je možné jej zohlednit ve smlouvě s dodavatelem. V takovém případě se totiž jedná o řízení dodavatelů, což je bezpečnostní opatření platné rovněž v režimu nižších povinností. Varování se tudíž musí zohlednit přiměřeně.

U osob, které nejsou regulované podle ZKB, varování nezakládá přímou zákonnou povinnost, ale představuje odborné doporučení. Tyto osoby (zadavatelé) tak sice nejsou povinny varování zohlednit, ale mohou (a typicky by měly) je dobrovolně promítnout do své analýzy rizik a interních pravidel, zejména pokud provozují služby významné pro společnost nebo veřejnou správu. Pokud jsou zadávací podmínky postaveny na řádně provedené analýze rizik, je omezení hospodářské soutěže přípustné i u zadavatelů, kteří nejsou regulovanou osobou.

1.3.3 Varování jako vstup do zadávacích podmínek

Pro tuto metodiku je podstatné, že varování je primárně vstupem do analýzy rizik, nikoli samo o sobě zadávací podmínkou ve smyslu § 28 odst. 1 písm. a) ZZVZ. Zadávací podmínky mají z varování vycházet zprostředkovaně přes výsledky řízení rizik a navazující bezpečnostní opatření podle § 13 a § 14 ZKB v souladu s příslušnou vyhláškou o bezpečnostních opatřeních (tj. ve vyšším či nižším režimu povinností).



Doporučený postup:

1) Zohlednění varování v analýze rizik

- zadavatel vyhodnotí, zda se hrozba popsaná ve varování týká poptávaného plnění (např. zda dané řešení pracuje s daty umisťovanými do rizikové lokality, využívá vzdálenou správu z rizikového území nebo zapojuje dodavatele, ke kterým se vztahuje varování),
- při hodnocení závažnosti hrozby vychází jednak z varování, jednak z vlastních znalostí prostředí a aktiv,
- zváží, zda je riziko akceptovatelné, nebo je nezbytné přijmout na základě § 13 a § 14 ZKB konkrétní přiměřené bezpečnostní opatření (přičemž takovým opatřením může být i omezení či vyloučení určitých technologií, dodavatelů nebo lokalit).

2) Promítnutí výsledků analýzy rizik do zadávací dokumentace

Výsledek analýzy rizik se následně může promítnout do zadávací dokumentace v rozsahu odpovídajícím povaze rizika a zvolenému způsobu jeho zvládání, typicky formou požadavků na:

- technické podmínky (vymezení předmětu plnění), včetně eliminace určitých technologií,
- kvalifikaci,
- dodavatelský řetězec, a vylučování určitých dodavatelů,
- hodnoticí kritéria,
- obchodní podmínky (smluvní ujednání), včetně případných sankcí a kontrolních mechanismů.

Tyto požadavky musí dodavatelé zohlednit v nabídce a po uzavření smlouvy budou v relevantním rozsahu závazné pro vybraného dodavatele. Bližší podrobnosti jsou uvedeny v kapitole 2 této metodiky.

Pokud je varování vydáno až po zahájení zadávacího řízení bude se konkrétní postup zadavatele odvíjet od fáze zadávacího řízení:

I. před podáním nabídek

Pokud to procesní situace umožňuje, zadavatel upraví zadávací podmínky tak, aby reflektovaly nově identifikovaná rizika, a to postupem podle § 99 ZZVZ. Současně přiměřeně prodlouží lhůty pro podání nabídek, aby dodavatelé mohli na změny reagovat. Následně zadavatel posuzuje splnění upravených podmínek a případně přistupuje k vyloučení dodavatelů, kteří je nesplní.

II. po podání nabídek

V této fázi je prostor pro změnu zadávacích podmínek omezený. Zadavatel proto posoudí, zda lze identifikovaná rizika řešit v rámci posouzení a hodnocení nabídek (např. prostřednictvím již stanovených požadavků nebo kritérií), případně zda je možné přijmout opatření až ve fázi plnění veřejné zakázky. Pokud by však uzavření smlouvy vedlo k nepřijatelnému bezpečnostnímu riziku, může zadavatel přistoupit ke zrušení zadávacího řízení podle § 127 ZZVZ.

> *V rozhodnutí ÚOHS ze dne 10. 3. 2026, sp. zn. ÚOHS-S0031/2026/VZ ÚOHS dospěl k závěru, že* ***v daném případě by postrádalo smyslu nutit zadavatele, aby pořídil plnění, jehož realizace by nutně znamenala ignorování varování NÚKIB ze dne 3. 9. 2025, a které by současně představovalo podstatné bezpečnostní riziko pro data, s nimiž zadavatel pracuje****. Tím spíše to platí v situaci, kdy jde o zadavatele (nemocnici) nakládajícího s osobními a citlivými údaji, které by měly požívat zvýšené míry ochrany. Je proto zřejmé, že zadavateli nelze vytýkat, že odmítl přijmout řešení, jež by mohlo ohrozit bezpečnost jeho dat, byť se do této situace dostal v důsledku vlastního pochybení při nastavení zadávacích podmínek.* ***Zadavatel objektivně identifikoval důvod hodný zvláštního zřetele pro zrušení zadávacího řízení až v průběhu zadávacího řízení (nikoli před jeho zahájením), a to ve spojení s obdržením nabídky navrhovatele.***

3) Proporcionalita a hospodářská soutěž

Omezení hospodářské soutěže plynoucí z promítnutí varování do zadávacích podmínek (např. omezení či vyloučení konkrétního typu technologie, způsobu provozu nebo lokality) lze uplatnit pouze tehdy, je-li:

- přímo odůvodněno výsledkem analýzy rizik provedené v souladu se ZKB a příslušnou vyhláškou o bezpečnostních opatřeních,

- nezbytné a přiměřené k dosažení požadované úrovně kybernetické bezpečnosti,
- formulováno transparentně a srozumitelně v zadávací dokumentaci.

Metodické materiály NÚKIB k varování z roku 2018 (Huawei/ZTE) a k varování ze dne 3. 9. 2025 obsahují konkrétní příklady, jak taková omezení formulovat v zadávací dokumentaci a jak je obhájit ve vztahu k právu veřejných zakázek.

> ***Povinnost správného hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik**, je akcentována např. v rozhodnutí ÚOHS ze dne 19. 2. 2024, sp. zn. ÚOHS-S0628/2023/VZ, č. j. ÚOHS-07501/2024/500.*
>
> *Jednalo se o veřejnou zakázku na zajištění modernizace ICT pro zvýšení kybernetické bezpečnosti, která byla zadávána společně několika nemocnicemi, z nichž žádná nebyla v té době povinnou osobou dle starého ZKB. ÚOHS posuzoval zákonnost bezpečnostní zadávací podmínky, kterou zadavatelé plošně vyloučili z plnění veřejné zakázky veškerá technická a programová řešení výrobců Huawei a ZTE, a to bez ohledu na povahu jednotlivých prvků plnění, jejich funkci, způsob začlenění či možnost alternativní mitigace rizik.*
>
> *Zadavatelé svůj postup odůvodňovali tím, že **dotčená zadávací podmínka je výsledkem řádně provedeného procesu řízení rizik** podle starého ZKB a bezpečnostní vyhlášky, a představuje jediné přiměřené opatření, jak snížit identifikovaná kybernetická rizika na akceptovatelnou úroveň. Úřad při posouzení věci vyšel mj. z analýzy rizik provedené zadavateli a vyžádal si rovněž odborné stanovisko NÚKIB, který potvrdil, že **provedená analýza rizik splňovala požadavky ZKB a vyhlášky**, dále že použití produktů Huawei/ZTE přináší nesnižitelná rizika, jejichž mitigace by byla nepřiměřeně nákladná, a rovněž že zadavateli stanovená bezpečnostní podmínka je přiměřená.*
>
> *Po posouzení věci Úřad dospěl k závěru, že **zadavatelé prokázali objektivní legitimní potřebu spočívající v zajištění kybernetické bezpečnosti u kritických ICT prvků, kdy se opřeli o dostatečně zpracovanou analýzu rizik**. Skutečnost, že zadavatelé nebyli formálně povinnými osobami dle § 3 starého ZKB, přitom dle ÚOHS nebrání dobrovolné aplikaci procesů a standardů ZKB a vyhlášky; proaktivní nastavení bezpečnostních opatření je tedy racionální a legitimní. Ze strany zadavatelů se tak dle závěrů rozhodnutí jednalo o nezbytné a přiměřené opatření k dosažení akceptovatelné úrovně rizika a nikoli o bezdůvodné omezení soutěže.*

Zadavatel nesmí nahrazovat analýzu rizik pouhou citací varování NÚKIB ani převzít varování jako samostatnou zadávací podmínku bez vazby na vlastní hodnocení rizik. Varování je vždy pouze vstupem do procesu řízení rizik podle ZKB. Teprve výsledky tohoto procesu mohou odůvodnit konkrétní bezpečnostní opatření a s nimi související omezení nebo požadavky v zadávacích podmínkách.

Naopak v rozhodnutí ze dne 25. 8. 2022, sp. zn. ÚOHS-S0196/2022/VZ ÚOHS dospěl k závěru, že v tomto konkrétním případě představovala zadávací podmínka spočívající ve vyloučení technických a programových prostředků některých výrobců ***nedovolenou diskriminaci a omezení hospodářské soutěže****.*

Úřad konstatoval, že zadavatel nemůže z plnění veřejné zakázky paušálně vyloučit veškeré technické a programové prostředky konkrétních výrobců ***pouze s odkazem na varování NÚKIB, pokud neprokáže, že takové omezení vychází z řádného, úplného a metodicky správného řízení rizik podle ZKB a bezpečnostní vyhlášky****. Nepředloží-li zadavatel dostatečnou analýzu rizik a neprokáže-li, že vyloučení je nezbytné a přiměřené, jde o bezdůvodnou překážku hospodářské soutěže. V šetřeném případě analýza rizik neproběhla v souladu se starým ZKB a metodikou NÚKIB, když příslušný dokument obsahoval pouze závěry, nikoli popis celého procesu analýzy rizik.*

Úřad proto uzavřel, že ***zadavatel neprokázal existenci rizik, jež by odůvodňovala absolutní zákaz technologií konkrétních výrobců****. V tomto smyslu lze také odkázat na rozhodnutí ÚOHS ze dne 13. 1. 2020 č. j. ÚOHS-S0358/2019/VZ-01269/2020/512/KMo, ve kterém Úřad označil obdobnou zadávací podmínku zadavatele ze nezákonnou, neboť zadavatel neprovedl řádné, metodicky správné a přezkoumatelné řízení rizik dle ZKB a bezpečnostní vyhlášky, když jeho analýza rizik byla nedostatečná a neodpovídající metodice NÚKIB; jako nedostatečná byla shledána zejména identifikace primárních a podpůrných aktiv, která by odůvodnila nezbytnost omezení soutěže o veřejnou zakázku, a vazeb mezi nimi. Vyloučení dodavatelů proto představovalo bezdůvodnou překážku hospodářské soutěže.*

1.3.4 Další nástroje NÚKIB jako vstupy do analýzy rizik (protiopatření)

Kromě varování mohou jako vstupy do analýzy rizik a následně do zadávacích podmínek sloužit také informace uvedené v reaktivním opatření podle § 23 ZKB či výstraze podle § 21. Kromě toho lze vycházet z právně nezávazných doporučení či neformálních upozornění zveřejňovaných průběžně na Portálu NÚKIB.

Z hlediska zadávání veřejných zakázek by měl zadavatel uvažovat stejným způsobem, jaký je popsán u varování. Nejprve zohlednit tato protiopatření, upozornění a doporučení v rámci analýzy rizik a bezpečnostní dokumentace podle ZKB. Teprve poté z nich odvodit konkrétní požadavky v zadávacích podmínkách, aby byla zajištěna návaznost mezi právní povinností v oblasti kybernetické bezpečnosti a omezeními či požadavky v zadávacím řízení.

1.4 Cíl metodiky: systematicky promítnout zajištění KB do veřejných zakázek

Hlavním cílem metodiky je prakticky propojit povinnosti zadavatele podle ZZVZ (transparentnost, nediskriminace, zákaz bezdůvodných překážek hospodářské soutěže), a povinnosti povinné osoby podle ZKB (řízení rizik, zavádění bezpečnostních opatření, řízení dodavatelů, reakce na varování a další protiopatření).

Metodika má zadavateli pomoci zejména:

1. převést výsledky analýzy rizik a dalších bezpečnostních procesů do podoby konkrétních zadávacích podmínek (technické požadavky, kvalifikace, kritéria hodnocení, smluvní ujednání),
2. zohlednit varování NÚKIB a další protiopatření v celém životním cyklu zakázky – od přípravy zadávací dokumentace až po kontrolu plnění,
3. najít přiměřenou rovnováhu mezi bezpečnostními požadavky a otevřenou hospodářskou soutěží,
4. dokumentovat a obhájit svůj postup vůči ÚOHS, soudům či kontrolním orgánům v případě, že jsou zadávací podmínky zpochybněny.

Zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti je nedílnou součástí řízení organizace a její kybernetické bezpečnosti. Odpovědnost za nastavení bezpečnostních požadavků a za přijatá rozhodnutí nelze přenést na dodavatele. Zadávací postupy musí navazovat na řízení rizik a bezpečnostní dokumentaci zadavatele a představují nástroj jejich praktické realizace.

Následující kapitoly metodiky (zejména kapitola 2) pak krok za krokem ukazují, jak tyto cíle naplnit v jednotlivých fázích zadávacího řízení a jak využít existující metodické materiály NÚKIB jako praktické „stavební kameny“ pro konkrétní zakázky.

2 Životní cyklus veřejné zakázky v oblasti ICT a kybernetické bezpečnosti

Kybernetická bezpečnost dnes prostupuje prakticky všemi oblastmi veřejné správy i veřejných služeb – nejen jako „ICT téma“, ale jako průřezová podmínka pro řádné fungování organizací, které jsou stále více závislé na digitálních systémech a jejich bezpečném fungování. V prostředí, ve kterém klíčové procesy využívají ICT, může mít zranitelnost zásadní dopady (zejména u kritické infrastruktury či řady digitalizovaných služeb veřejné správy, významných pro chod státu a jeho institucí). Tím se přirozeně zvyšuje tlak na systematické nastavování bezpečnostních standardů a jejich skutečné naplňování.

Tento tlak se promítá i do zadávání veřejných zakázek. Zadavatel totiž v oblasti ICT a kybernetické bezpečnosti jen nenakupuje určitý produkt nebo službu, ale zajišťuje si (a často dlouhodobě provozuje) schopnost plnit bezpečnostní cíle a povinnosti, a to velmi často s využitím veřejných prostředků. Vedle požadavků na funkčnost a kontinuitu se proto v celém životním cyklu zakázky nevyhnutelně uplatní i **principy účelnosti, hospodárnosti a efektivnosti** (3E) a **obecné zásady zadávání veřejných zakázek**.

Specifikem veřejných zakázek v oblasti ICT a kybernetické bezpečnosti je, že vhodné řešení se nedá univerzálně předepsat a určit jediným technickým či bezpečnostním checklistem. Smysluplný start přípravy zadávacího řízení by vždy měl vycházet z dobrého vymezení (zmapování) potřeb zadavatele a jím prováděného rozsahu řízení kybernetické bezpečnosti, tj. z pochopení aktiv a rizik v konkrétním prostředí zadavatele a ve volbě odpovídajících bezpečnostních opatření (organizačních i technických). Teprve z tohoto základu lze odvodit vhodné zadávací podmínky, vymezit legitimní požadavky na plnění a například i vhodně řídit řetězec dodavatelů.

Praktickým důsledkem je, že zadavatelé veřejných zakázek v oblasti ICT a kybernetické bezpečnosti musí své kyberbezpečnostní požadavky promítat konzistentně nejen do přípravy a průběhu zadávacího řízení, ale i do **celé smluvní fáze, implementace řešení, zajištění jeho provozu, změnového řízení a ukončení plnění** (včetně exit plánu s opatřeními proti vendor lock-in, jako je např. předání dokumentace a dat, zajištění přenositelnosti licencí, součinnost při převzetí provozu jiným dodavatelem nebo stanovení podmínek ukončení a předání služby).

Zadavatelům veřejných zakázek lze proto doporučit systematický přístup od počáteční identifikace potřeby a rizik, přes volbu vhodného druhu zadávací řízení, formulaci zadávacích podmínek, až po řízení plnění, kontrolu bezpečnostních parametrů a zvládání incidentů či změn.

2.1 Příprava a analýza potřeb zadavatele, ověření formou předběžné tržní konzultace a volba postupu

V oblasti ICT a kybernetické bezpečnosti je přípravná fáze klíčová, protože rozhoduje o tom, zda zadavatel dokáže vhodně přenést své potřeby do zadávacích podmínek tak, aby výsledkem nebylo pouze formálně správně vysoutěžené řešení, ale také funkční a bezpečné plnění. Už v přípravné fázi

je třeba pracovat s tím, že bezpečnostní opatření, která zadavatel promítne do zadávacích podmínek, budou často znamenat určité omezení hospodářské soutěže.

> *Zadávací podmínky, které mohou omezovat hospodářskou soutěž, musí být ze strany zadavatele vždy odůvodněny nejen věcně (legitimní cíl), ale rovněž optikou zásady přiměřenosti ve smyslu **tříkrokového testu proporcionality**:*
>
> *1) vhodnost – vede opatření k dosažení cíle?*
> *2) potřebnost – nelze dosáhnout cíle mírnějšími prostředky?*
> *3) přiměřenost v užším smyslu – obstojí omezení v kolizi s jinými právy a zájmy?*
>
> *Zadavatel je povinen přiměřenost omezujících zadávacích podmínek posuzovat s ohledem na povahu veřejné zakázky, situaci na trhu a existenci alternativ, které by vedly ke stejnému cíli s menším dopadem na hospodářskou soutěž (srov. rozsudek Nejvyššího správního soudu ze dne 16. 6. 2025, č. j. 3 As 120/2024-81.*

Aby taková omezení byla legitimní a legální, musí být racionální, odůvodněná potřebami zajištění bezpečnosti ICT a přiměřená; současně platí, že zohlednění požadavků vyplývajících z bezpečnostních opatření v nezbytné míře nelze považovat za nezákonné omezení soutěže o veřejnou zakázku (tj. porušení ZZVZ).

> *Stanovení takových omezujících zadávacích podmínek nepředstavuje libovůli zadavatele, nýbrž způsob, jak zadavatel může dostát svým zákonným povinnostem v oblasti kybernetické bezpečnosti. Zadavatel je povinen se při zadávání veřejných zakázek řídit právním řádem České republiky jako celkem. Nemůže-li tak zadavatel dodržet svou zákonnou povinnost při zadávání veřejné zakázky v oblasti kybernetické bezpečnosti jinak, než přijetím určitého opatření, nejedná se o nedovolenou diskriminaci, neboť takový závěr by vedl k situaci, kdy by zadavatel předmět veřejné zakázky vůbec nemohl poptat (viz např. rozhodnutí ÚOHS ze dne 6. 11. 2019, sp. zn. S0262/2019/VZ, č. j. ÚOHS-S0262/2019/VZ-30266/2019/523/JMa).*

Zadavatel by měl před zahájením zadávacího řízení zvážit a mít k dispozici zejména:

- **popis potřeb a cílového stavu** (co má řešení umožnit, jaké procesy podporuje),
- **vymezení chráněných aktiv a dopadů** (co je kritické, jaké jsou požadavky na důvěrnost, integritu, dostupnost),
- **analýzu rizik a návrh jejich mitigace** (v míře adekvátní významu poptávaného plnění a dopadům případného selhání),
- **návrh zadávací strategie** (jaké instrumenty ZZVZ lze vhodně využít pro přenesení bezpečnostních potřeb a požadavků do zadávacích podmínek),
- **zdůvodnění volby postupu** (interní úvaha zadavatele, zda postačí zadávací řízení bez jednacího prvku, anebo je vhodnější zvolit vícefázová řízení s jednacím prvkem).

Uvedený výčet představuje minimální rámec úvah, které by měl zadavatel před zahájením zadávacího řízení provést. Míra podrobnosti a formálního zachycení jednotlivých kroků by měla být přiměřená rozsahu, složitosti a rizikovosti poptávaného plnění. V praxi to znamená, že u méně významných nebo standardizovaných plnění (např. zakázky malého rozsahu nebo plnění s nízkým dopadem na primární aktiva) může postačovat zjednodušená analýza rizik a stručnější dokumentace. Naopak u zakázek s významným dopadem na poskytování regulované služby nebo na bezpečnost primárních aktiv je nezbytné provést analýzu rizik v odpovídající hloubce a zajistit její řádné zdokumentování.

Pro lepší představu lze uvést příklad minimálního rozsahu dokumentace či interního zachycení těchto úvah. Takový podklad může mít podobu jednoduchého dokumentu, tabulky nebo interní poznámky. Zadavatel může mít k dispozici například stručný podklad obsahující:

1. identifikaci dotčených **aktiv** (primárních a podpůrných),
2. přehled hlavních **zjištěných rizik** (včetně jejich orientační závažnosti),
3. **zvolená opatření** ke snížení rizik,
4. promítnutí těchto opatření do **zadávacích podmínek** a volby zadávacího postupu.

Shora uvedené nemusí být součástí samostatných (formálních) dokumentů, když místo formy je stěžejní, že zadavatel úvahy v uvedeném rozsahu provedl, tj. shora uvedenými aspekty se před zahájením zadávacího řízení zabýval. Bez ohledu na rozsah dokumentace však platí, že zadavatel musí být schopen zejména před ÚOHS pro účely posouzení souladnosti postupu s relevantními právními předpisy, uvedené zpětně doložit.

Ačkoli výsledky analýzy rizik a navazující rozhodnutí zpravidla nejsou součástí zadávací dokumentace ani nejsou veřejně zpřístupňovány, měl by mít zadavatel jednotlivé úvahy, závěry a zvolená opatření řádně zdokumentované a dohledatelné. Taková dokumentace slouží zejména k interní kontrole, auditu a k obhajobě postupu zadavatele v případě přezkumu, zejména z hlediska posouzení, zda omezení hospodářské soutěže vyplývalo z legitimních povinností podle ZKB a bylo přiměřené sledovanému cíli.

Analýza potřeb zadavatele (co zadavatel skutečně pořizuje) a rizik plnění (v jádru jde o vyhodnocení dopadů kombinace hrozeb a zranitelností vůči chráněným aktivům a o určení úrovně rizika na stupnici nízké až kritické) je základem pro návaznou práci se zadávacími podmínkami. Po identifikaci rizik musí následovat volba konkrétních opatření (mitigací), kterými zadavatel sníží riziko na akceptovatelnou úroveň. Z pohledu veřejného zadávání je klíčové, aby se závěry analýzy rizik a přijatých opatření ke zmírnění rizik „propsaly“ do zadávacích podmínek prostřednictvím vhodných nástrojů ZZVZ (např. technické podmínky, požadavky na kvalifikaci, hodnotící kritéria, smluvní podmínky). Současně je třeba pamatovat, že nesprávné nastavení zadávacích podmínek může vést k oslabení bezpečnostních opatření, neefektivnímu nastavení systémů v prostředí zadavatele, nebo dokonce k jejich nefunkčnosti. Nezákonné nastavení zadávacích podmínek může vést až ke zrušení celého zadávacího řízení a k nutnosti realizovat celý proces znovu, což v důsledku znamená vynaložení dalších personálních, časových i finančních kapacit navíc, a to bez zajištění předmětu plnění – což je cílem celého zadávacího procesu.

Zadavatel může zvážit vhodnost ověření, proveditelnost a přiměřenost požadavků ještě před zahájením zadávacího řízení (bez ohledu na to, zda veřejná zakázka má být zadávána v jednofázovém řízení či v zadávacích řízeních s jednacím prvkem). K tomu slouží **předběžné tržní konzultace** dle § 33 ZZVZ (dále jen „PTK"). Zadavatel je oprávněn vést PTK s odborníky či dodavateli za účelem přípravy zadávacích podmínek a informování trhu o záměrech a požadavcích, přičemž tento postup je třeba realizovat způsobem nenarušujícím hospodářskou soutěž a z důvodu transparentnosti je nutné jej zdokumentovat, a promítne-li se do stanovení zadávacích podmínek, je třeba tuto skutečnost v zadávací dokumentaci uvést, resp. identifikovat osoby, které se na PTK podílely, a v souladu s § 36 odst. 4 věta druhá ZZVZ označit konkrétní části zadávací dokumentace, vycházející z PTK.

Dle okolností konkrétní situace má PTK v kontextu kybernetické bezpečnosti typicky tyto praktické cíle:

> *V této souvislosti lze dále odkázat např. na rozsudek Nejvyššího správního soudu č. j. 5 As 340/2022-84 ze dne 15. 12. 2023, dle jehož **závěrů lze PTK využívat nejen před zahájením zadávacího řízení, ale i v jeho průběhu, pokud směřují k přípravě či změně zadávacích podmínek**. Jakákoli komunikace s dodavateli, která má reálný vliv na jejich obsah, musí být považována za PTK. Zadavatel je povinen v souladu s § 36 odst. 4 ZZVZ transparentně označit části zadávací dokumentace ovlivněné PTK a uvést subjekty, které se na jejich přípravě podílely. Zároveň z cit. rozsudku vyplývá, že změny zadávacích podmínek učiněné na základě PTK musí být řádně odůvodněny z hlediska jejich přiměřenosti a skutečných potřeb zadavatele.*

1. **Zmapování trhu** – v případech, kdy zadavatel nemá dostatečné znalosti o relevantním trhu, mohou PTK sloužit k získání přehledu o dostupných řešeních a jejich funkcionalitách.
2. **Zpřesnění rozsahu plnění** – vlastní obsah a definovaná hloubka technického řešení, rozsah implementace a podpory, reakční doby a SLA režimy, reálná doba plnění, délka záruky a doba trvání smlouvy aj.
3. **Validace požadavků zadavatele/zadávacích podmínek** – co je považováno za tržní standard, četnost výskytu referencí technické kvalifikace nebo certifikátů členů týmu, co je specifické a z jakého důvodu (a zda možná řešení jsou způsobilá uspokojit potřeby zadavatele); možnost ověření a úpravy zadávacích podmínek na základě zpětné vazby od účastníků PTK,
4. **Ověření variant architektury** – on-premise řešení/cloud/hybridní model, integrační vazby, licenční modely aj.,
5. **Podklady pro předpokládanou hodnotu veřejné zakázky/Total Cost of Ownership (TCO) -** lze ověřit nákladovost poptávaného řešení, nejen cenu vlastní implementace, ale celé náklady životního cyklu a budoucí provozní náročnosti zamýšleného řešení. Ještě před vlastním návrhem zadávací strategie musí zadavatel stanovit předpokládanou hodnotu (§ 16 ZZVZ), protože od ní se odvíjí režim veřejné zakázky (§ 24 ZZVZ) a následně i volba použitelných postupů (podlimitní/nadlimitní, druh zadávacího řízení).

Veřejné zakázky v oblasti ICT a kybernetické bezpečnosti často vyžadují, aby zadavatel pracoval s interními předpisy a dokumentacemi popisujícími konkrétní systémy a jejich zabezpečení. Jejich poskytování třetím osobám může samo o sobě představovat významné bezpečnostní riziko, protože může poukázat na slabiny technického či organizačního zabezpečení. Typicky se může jednat například o dokumentaci architektury informačních systémů, seznamy aktiv, identifikované zranitelnosti, detailní konfigurace systémů nebo plány řešení bezpečnostních incidentů. Pokud zadavatel poskytuje tyto důvěrné informace již v rámci PTK, je oprávněn je zpřístupnit konzultujícím dodavatelům ve specifickém režimu, aby byla zajištěna jejich ochrana (blíže viz kapitola 2.4).

Doporučený postup PTK v zakázkách kybernetické bezpečnosti:

- zadavatel předem definuje okruhy otázek (např. bezpečnostní standardy, funkční a nefunkční požadavky, SLA, integrace, požadavky na kvalifikaci, způsob hodnocení nabídek, systém poddodávek, exit strategie aj.),
- zadavatel zvolí formu PTK (RFI/dotazník; workshop; případně série/kola konzultací ať už v písemné, ústní či kombinované formě),
- zadavatel vyhodnotí získané informace a promítne je do zadávacích podmínek („must have“ požadavky vs. „nice to have“ požadavky), přičemž získané informace zadavatel zhodnotí kriticky při vědomí, že PTK nesmí vést ke skryté preferenci konkrétního řešení (např. bezpečnostní požadavky formulované „na míru“ konkrétnímu dodavateli bez legitimního důvodu),
- zadavatel pořídí záznam o provedených PTK a zajistí, aby v zadávací dokumentaci byly označeni dodavatelé, kteří se na PTK podíleli, resp. byly označeny osoby, které mají přičitatelný a přímý podíl na obsahu příslušné části zadávací dokumentace, a to vždy ve vztahu ke konkrétní části zadávací dokumentace.

2.2 Zadávací řízení s jednacím prvkem

Volba postupu: kdy postačí řízení bez jednacího prvku a kdy je vhodný jednací prvek

Volba druhu zadávacího řízení má v oblasti ICT a kybernetické bezpečnosti přímý dopad na to, v jaké fázi může zadavatel své bezpečnostní požadavky doplňovat a zpřesňovat.

Řízení bez jednacího prvku (typicky otevřené řízení, zjednodušené podlimitní řízení, užší řízení) neumožňuje jednání před podáním nabídky, ani o obsahu nabídky a po uplynutí lhůty pro podání nabídek nelze připustit změny či doplnění zadávacích podmínek ani nabídek (v materiálním smyslu). To znamená, že veškeré procesy zohlednění bezpečnostních požadavků musí být předem zakotveny v zadávací dokumentaci.

*V souvislosti s tématem **dovolených či nedovolených změn nabídek** lze odkázat např. na rozhodnutí předsedy ÚOHS č. j. ÚOHS-07119/2021/161/TMi ze dne 2. 3. 2021 či rozhodnutí Úřadu č. j. ÚOHS-02686/2021/500/AIV ze dne 22. 1. 2021 nebo rozsudek Nejvyššího správního soudu č. j. 9 As 7/2022-85 ze dne 3. 4. 2024.*

Naopak **řízení s jednacím prvkem** (zejména jednací řízení s uveřejněním – JŘSU, anebo řízení se soutěžním dialogem) mohou být ve veřejných zakázkách v oblasti ICT a kybernetické bezpečnosti vhodně využitelné. Pokud potřeby zadavatele nelze uspokojit bez úpravy plnění dostupných na trhu, součástí plnění je návrh/inovativní řešení, nebo je zakázka z povahy či složitosti spojena se zvláštními okolnostmi, je zadavatel oprávněn využít JŘSU, ve kterém může postupně „filtrovat" vážné zájemce a poskytovat informace průběžně podle fází zadávacího řízení. Řízení se soutěžním dialogem je určeno zejména pro situace, kdy zadavatel nezná vhodné řešení a společně s účastníky jej teprve hledá; bezpečnostní aspekty mohou být předmětem jednání a citlivé informace lze opět poskytovat postupně v závislosti na fázi tohoto zadávacího řízení. Z praktického hlediska spočívá největší rozdíl mezi JŘSU a řízením se soutěžním dialogem v existenci tzv. minimálních technických podmínek. Podle ustanovení § 61 odst. 4 ZZVZ v případě JŘSU platí, že "*V zadávací dokumentaci zadavatel označí, které požadavky na plnění veřejné zakázky představují minimální technické podmínky, které musí nabídka splňovat*." Tyto minimální technické podmínky jsou dané a nezměnitelné, zadavatel již o nich v průběhu zadávacího řízení nemůže jednat. Oproti tomu pravidla pro použití řízení se soutěžním dialogem dle § 69 ZZVZ s existencí minimálních technických podmínek nepočítají, ustanovení detailních parametrů předmětu veřejné zakázky je tedy více autonomní a může být téměř bezvýhradně koordinováno až během jednacích fází řízení.

Specifickou vlastností řízení s jednacím prvkem je skutečnost, plynoucí z § 36 odst. 2 ZZVZ – "*Zadávací podmínky zadavatel uvede v zadávací dokumentaci nebo ve výzvě uvedené v příloze č. 6 k tomuto zákonu anebo je sdělí účastníkům zadávacího řízení při jednání.*". Právě sdělení určité části zadávacích podmínek až omezenému okruhu účastníků při jednání je jednou ze zásadních výhod, které kompenzují nutnost zadavatele "předvídat" veškerá možná nabídnutá řešení již před zahájením řízení a vůči tomu nastavit zadávací podmínky dostatečně široce, jako je tomu u řízení bez jednacího prvku. Z všeobecné variability technických řešení je možné konstatovat, že každé řešení vyžaduje odlišný charakter vstupů (např. informace o stávající infrastruktuře a systémech, popis jejich fungování, existence rozhraní či konektorů, licenční omezení konkrétní komponenty apod.). V řízení bez jednacího prvku musí zadavatel počítat v podstatě se všemi hypotetickými možnostmi řešení, případně se spolehnout na to, že na dílčí detaily položí dodavatelé dotazy v rámci žádosti o vysvětlení zadávací dokumentace dle § 98 ZZVZ. Tento institut však nemůže nahradit řádné stanovení zadávacích podmínek v souladu s § 36 odst. 1 a 3 ZZVZ. Oproti tomu v řízení s jednacím prvkem lze uvedené dílčí detaily sdělit konkrétnímu dodavateli v rámci jednací fáze, v komplementárním souladu s jím zamýšleným návrhem konkrétního řešení, a následně tuto informaci předat i dalším účastníkům jednací fáze (s naplněním zásady rovného přístupu). Tento postup zajišťuje flexibilitu zadavatele a snižuje nároky na hloubku odbornosti zadávacích podmínek, jakou by zadavatel musel užít v rámci řízení bez jednacího prvku.

Mezi informace, které mohou být v řízení s jednacím prvkem sděleny až konkrétním účastníkům při jednání, mohou patřit popisy stávajícího prostředí, údaje o analýze rizik, výčet bezpečnostních opatření apod. Může tedy jít o údaje velice citlivého charakteru, které takto v řízení s jednacím prvkem zadavatel předává pouze omezenému počtu (důvěryhodných) účastníků, oproti řízení bez jednacího prvku, kde by tyto informace byly zpřístupněny neomezenému okruhu účastníků na profilu zadavatele, anebo byly vydávány s vyšší administrativní náročností v průběhu lhůty pro podání nabídek oproti dohodě o mlčenlivosti. I z hlediska kybernetické bezpečnosti tedy použití řízení s jednacím prvkem může nabídnout procesní výhodu.

Praktické rozhodovací pravidlo pro volbu postupu lze shrnout takto:

- pokud zadavatel umí (po analýze rizik a případných PTK) popsat předmět plnění a bezpečnostní požadavky dostatečně přesně a nepotřebuje dále „ladit" řešení s trhem, je možné zvolit řízení bez jednacího prvku; toto klade vyšší nároky na kvalitu zadávací dokumentace od samého počátku zadávacího řízení.
- pokud jde o komplexní řešení s významnou nejistotou (customizace, inovace, komplikované podmínky, potřeba postupného zpřesňování informací), je na místě zvažovat využití JŘSU či řízení se soutěžním dialogem, a to i s ohledem na možnou ochranu důvěrných informací a efektivní práci s riziky.

Do řízení s jednacím prvkem řadíme ještě **jednací řízení bez uveřejnění** (JŘBU), v němž dochází k přímé výzvě k podání nabídky nebo k zahájení jednání (zpravidla) jednomu dodavateli. Pro použití JŘBU platí specifické restriktivní podmínky, definované v § 63 ZZVZ. Z pohledu veřejných zakázek v oblasti ICT a kybernetické bezpečnosti je pak dále možné rozlišovat dvě situace, za nichž je možno o využití JŘBU uvažovat, do nichž bezprostředně vstupují technicko-technologická specifika tohoto odvětví:

- JŘBU, v němž jsou podmínky „exkluzivity" dle § 63 odst. 3 písm. b) nebo c) ZZVZ naplněny nezávisle na zadavateli, např. tedy
  - v důsledku přirozeného stavu trhu, kdy určité plnění dodává pouze jediný dodavatel, anebo
  - jediný dodavatel je určen nezávisle na zadavateli resortním právním předpisem nebo jiným obdobným dokumentem,
- JŘBU, u něhož je naplnění podmínky „exkluzivity" dáno předchozím jednáním zadavatele, tj. tzv. JŘBU ve stavu vendor lock-in, typicky např. pořízení informačního systému a následné omezení jeho dalšího rozvoje na původního dodavatele – vendora. V této situaci jsou možnosti legálního využití JŘBU extrémně limitované. Rámec podmínek, za kterých je možno o využití JŘBU v těchto případech uvažovat, je definovaný dnes již poměrně obsáhlou judikaturou a zmiňovaný ve specifických metodikách. Velmi zjednodušeně řečeno jde zejména o materiální podmínku spočívající v tom, že zadavateli není stav exkluzivity přičitatelný, která je naplněna jen za předpokladu, že zadavatel v době, kdy stav exkluzivity založil, nemohl rozumně předpokládat potřebu zadávání dalších navazujících veřejných zakázek, a zároveň že stav exkluzivity neudržoval poté, co potřebu navazujícího plnění zjistil, ačkoli měl k dispozici prostředky k jeho ukončení.

K tématu možnosti využití JŘBU existuje bohatá judikatura, kdy lze odkázat např. na jeden z nedávných rozsudků Nejvyššího správního soudu ze dne 6. 2. 2025, č. j. 8 As 314/2021 - 123, z něhož vyplývá, že ***ani skutečnost, že zadavatel v době uzavření původní smlouvy nemohl předvídat vznik budoucí závislosti na jediném dodavateli, sama o sobě neodůvodňuje použití JŘBU*** *– rozhodující je, zda zadavatel stav exkluzivity udržoval i v době, kdy jeho další trvání bylo již z hlediska aktuální právní úpravy nežádoucí, a zda měl k dispozici skutečné a z finančního hlediska přiměřené prostředky k jeho ukončení.*

Rovněž lze upozornit též na rozsudek Nejvyššího správního soudu ze dne 8. 2. 2023, č. j. 1 As 176/2022-99,, v němž se soud zabýval otázkou, zda zadavatel při zadávání veřejné zakázky na upgrade informačního systému naplnil podmínky pro použití JŘBU dle § 63 odst. 3 písm. c) ZZVZ. Při posuzování otázky, zda je stav exkluzivity přičitatelný zadavateli, pokud byl založen v minulosti, soud připustil, že ***dnešní pravidla práva veřejných zakázek nelze zpětně vztahovat na iniciační smlouvy uzavřené v dávné minulosti****; tato skutečnost však sama o sobě neospravedlňuje trvající stav exkluzivity. V šetřené věci byl tento stav udržován a opakovaně prohlubován uzavíráním následných dodatků, aniž by zadavatel podnikl jakékoli kroky k jeho omezení či odstranění. Zadavatel tak setrvával ve „stavu pohodlí" a dále rozšiřoval funkcionality kdysi pořízeného informačního systému, ačkoli již při jeho pořízení bylo jisté, že jej bude nutné v budoucnu dále rozvíjet. Soud připomněl, že JŘBU je mimořádný postup, který nelze odůvodňovat pouze historickými smluvními vztahy, a to zejména v oblasti ICT, kde je třeba zvýšené opatrnosti při uzavírání dlouhodobých smluv.*

2.3 Zadávací dokumentace – technické a bezpečnostní požadavky

Povinnost zavádět (preventivní) bezpečnostní opatření pro zvýšení odolnosti organizace je podstatou existence ZKB. Zatímco poskytovatelé služeb v režimu vyšších povinností zavádějí bezpečnostní opatření systematickým přístupem založeným na práci s riziky, v případě poskytovatelů služeb v režimu nižších povinností se jedná o povinnost zavádět zjednodušená bezpečnostní opatření. Bez ohledu na režimový status osoby dle ZKB mají všichni zadavatelé prostor zohlednit požadavky vyplývající z bezpečnostních opatření, jak ukládá § 13 odst. 2 ZKB, v rámci technických podmínek podle § 37 odst. 1 písm. b) ZZVZ, resp. § 89 ZZVZ v případě nadlimitního režimu.

Obecně je problematika technických podmínek veřejných zakázek zadávaných v nadlimitním režimu upravena § 89 odst. 1 ZZVZ, kterým je stanoveno, že „*Technické podmínky jsou požadavky na vlastnosti předmětu veřejné zakázky, které zadavatel stanoví prostřednictvím a) parametrů vyjadřujících požadavky na výkon nebo funkci, popisu účelu nebo potřeb, které mají být naplněny, b) odkazu na normy nebo technické dokumenty, nebo c) odkazu na štítky.*" Technické podmínky veřejné zakázky jsou obvykle obsaženy v příloze „technická specifikace" (nicméně příslušná část zadávací dokumentace může být nazvána i jinak, příp. se vůbec nemusí jednat o samostatnou přílohu, ale dané zadávací podmínky mohou být inkorporovány přímo do „těla" zadávací dokumentace), v níž jsou tyto podmínky uvedeny formou integrovaného celku požadavků. Tento dokument je defacto primární součást zadávací dokumentace (předmět veřejné zakázky, vyplývající z potřeb zadavatele

je důvodem realizace zadávacího řízení), a musí být v zájmu dodržení § 36 ZZVZ jasný a srozumitelný pro každého účastníka zadávacího řízení.

Bezpečnostní požadavky by měly být formulovány funkčně, tedy co musí řešení zajistit, a nikoli technologicky, tedy jaké konkrétní řešení použít. Tímto se minimalizuje riziko přímých a nepřímých odkazů a zvýší se možnost konkurence.

Pokud se v rámci technické specifikace objevují tzv. přímé nebo nepřímé odkazy na určité dodavatele nebo výrobky, nebo na patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, lze to akceptovat jen v souladu s § 89 odst. 5 ZZVZ (odkaz je odůvodněn předmětem veřejné zakázky), ve specifických případech pak § 89 odst. 6 ZZVZ (stanovení technických podmínek podle § 89 odst. odst. 1 ZZVZ nemůže být dostatečně přesné nebo srozumitelné). Jedná se ovšem o výjimky z obecného postupu, tzn. že při zvažování ohledně jejich aplikace je třeba postupovat spíše restriktivně.

Na aplikovatelnost pravidla dle § 89 odst. 5 ZZVZ by mělo být pohlíženo obdobně striktní optikou jako na možnost zadavatele postupovat v JŘBU ve smyslu § 63 odst. 3 písm. b) ZZVZ, k tomu srov. rozhodnutí předsedy ÚOHS ze dne 29. 3. 2019, č. j. ÚOHS-R0022/2019/VZ-09006/2019/322/JSu).

*V rozsudku Nejvyššího správního soudu ze dne 23. 6. 2025, č. j. 1 As 57/2025-27 je dovozeno, že konkrétní odkaz na plnění veřejné zakázky lze použít ve dvou situacích. Buď **může být veřejná zakázka nevyhnutelně splněna jedním jediným plněním**, a proto nelze připustit ani alternativy (§ 89 odst. 5 ZZVZ). Anebo **není možné popsat technické podmínky dostatečně přesně a srozumitelně, pročež zákon připouští odkaz na konkrétní plnění** (či příkladmý výčet) s tím, že zadavatel výslovně připustí rovnocenné plnění (§ 89 odst. 6 ZZVZ). Jelikož každá výjimka vychází z jiného předpokladu, je zřejmé, že jejich použití se navzájem vylučuje. Buď je předmět zakázky natolik specifický, že nemůže být uspokojen ničím jiným než jedním konkrétním plněním. Anebo jej nelze dostatečně popsat obecným způsobem, a proto lze odkázat na konkrétní plnění a připustit rovnocenné plnění.*

Přímým odkazem je myšleno výslovné uvedení názvu výrobku, výrobce, dodavatele, nebo trademark specifické technologie. Nepřímým odkazem je pak specifická technická podmínka, nebo kombinace technických podmínek, která se na první pohled jeví obecně, ale svým věcným reálným obsahem ke konkrétnímu výrobku, výrobci, dodavateli či technologii tak, jako by byl uveden přímý odkaz.

Obecně požadavek na produkt či službu konkrétního výrobce představuje omezení hospodářské soutěže, přičemž mnohdy je takové omezení nežádoucí. Situace, kdy zadavatel bude zvažovat důvodnost použití přímého či nepřímého odkazu v oblasti ICT a kybernetické bezpečnosti může být poměrně častá. Běžně se jedná o požadavky, kdy je vyžadována určitá konkrétní HW či SW komponenta z důvodů dodržení kompatibility se stávajícím řešením (např. server, switch, virtualizační nástroj, firewall apod.). V takovém případě může být s ohledem na předmět veřejné zakázky hospodářská soutěž v oblasti konkrétní komponenty omezena na konkrétního výrobce (technologickou platformu), z globálního hlediska je však hospodářská soutěž ve většině případů

stále možná mezi dodavateli (distributory) konkrétního výrobce, a mezi generálními dodavateli kompletního řešení. Odůvodnění předmětem veřejné zakázky se rovněž může dotýkat situace, kdy je konkrétní odkaz podmíněn např. uživatelskou kompatibilitou (např. zaměstnanci pracují s určitým operačním systémem), legislativním doporučením (např. použitím konkrétních kryptografických prostředků), nepoužitelností jiných řešení na trhu apod., avšak zadavatel je vždy povinen pečlivě zvážit, zda omezení soutěže je legitimní jako důsledek charakteru daného plnění, a nikoliv nelegitimní, neprozíravý či dokonce účelový postup zadavatele. Zadavatel musí být vždy schopen použití konkrétního odkazu argumentačně obhájit, jakkoli takové odůvodnění nemusí být součástí samotné technické specifikace.

Z pohledu průběhu hospodářské soutěže o konkrétní veřejnou zakázku je nutné brát v potaz, že pokud je hospodářská soutěž o předmět veřejné zakázky, který je vymezen mj. prostřednictvím z jednoho či více přímých nebo nepřímých odkazů, stále možná mezi dodavateli konkrétního výrobce, nebo generálními dodavateli, pak zadavatel může důvodně očekávat, že je schopen obdržet dvě a více nabídek. Pokud však přímé či nepřímé odkazy vedou do situace, kdy je nabídku schopen podat pouze jediný dodavatel (např. jediný distributor konkrétního výrobce v rozsahu všech poptávaných komponent), pak se jedná o podmínky, kdy veřejná zakázka může být splněna pouze určitým dodavatelem. Za splnění specifických podmínek dle § 63 odst. 3 ZZVZ pak zadavatel může v konkrétní situaci zvažovat zadávací postup v JŘBU.

Technické podmínky podle § 36 odst. 1 ZZVZ samozřejmě nesmí bezdůvodně vytvářet překážky hospodářské soutěže. To zahrnuje i zákaz neodůvodněného slučování plnění, která běžně dodávají různí dodavatelé (tzv. diskriminační slučování). Ve veřejných zakázkách v oblasti ICT a kybernetické bezpečnosti se může jednat například o spojování fyzických bezpečnostních opatření (např. stavební či elektrotechnické práce) s dodávkami HW/SW nebo implementačními službami bez věcného odůvodnění.

2.4 Ochrana důvěrných informací v průběhu zadávacího řízení

2.4.1 Povaha důvěrných informací v oblasti ICT a kybernetické bezpečnosti

Zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti je zpravidla spojeno s prací s informacemi, jejichž zpřístupnění neoprávněným osobám může samo o sobě představovat významné bezpečnostní riziko. Typicky se jedná o informace o architektuře informačních systémů, jejich konfiguraci, provozních vazbách, bezpečnostních opatřeních, identifikovaných rizicích či zranitelnostech. V některých případech mohou být tyto informace součástí bezpečnostní dokumentace vedené podle ZKB nebo prováděcích právních předpisů, případně mohou souviset s ochranou osobních údajů, utajovaných informací či obchodního tajemství.

Poskytování těchto informací třetím osobám může představovat výrazné bezpečnostní riziko, neboť může odhalit potenciálním útočníkům slabiny technického či organizačního zabezpečení informačního nebo komunikačního systému, včetně konkrétních technologií, které jsou využívány, a způsobu jejich nastavení. Z tohoto důvodu musí být zadavatelé schopni tyto informace účinně chránit před neoprávněným zpřístupněním nebo dalším šířením.

2.4.2 Transparentnost a ochrana důvěrných informací

Zadavatel je v průběhu zadávacího řízení povinen hledat rovnováhu mezi zásadou transparentnosti podle ZZVZ a povinností chránit důvěrné informace, která mu vyplývá, jak z obecné povinnosti jednat s péčí řádného hospodáře, tak z konkrétních právních předpisů v oblasti kybernetické bezpečnosti. Transparentnost zadávacího řízení neznamená povinnost bez dalšího zpřístupňovat veškeré informace všem potenciálním dodavatelům. Právní úprava naopak vychází z toho, že zadavatel je oprávněn, a v řadě případů povinen, určité informace chránit, pokud by jejich zveřejnění bylo v rozporu s jeho legitimními zájmy nebo by vedlo k ohrožení bezpečnosti.

> *Přímo v kontextu kybernetické bezpečnosti lze odkázat na rozsudek Nejvyššího správního soudu ze dne 25. 9. 2019, č. j. 6 As 113/2019-32. Soud se v řízení o kasační stížnosti zabýval situací, kdy zadavatel při zadávání veřejné zakázky požadoval po **dodavatelích předložení konkrétního certifikátu managementu bezpečnosti informací**. Soud konstatoval, že předmětný požadavek zadavatele měl souvislost s předmětem veřejné zakázky, neboť součástí předmětu plnění byl mj. servis přístrojů obsahujících záznamy údajů týkajících se důležitých osobních informací. Vybraný dodavatel se tak mohl dostat k citlivým údajům, na jejichž ochranu je kladen čím dál větší důraz. U technologií, které ukládají nebo přenášejí osobní data, má zavedení takového systému přímou vazbu na kvalitu plnění, protože ovlivňuje bezpečnost provozu a integritu dat. **Daný požadavek zadavatele tak byl dle soudu racionální a legitimní.***

Specifika veřejných zakázek v oblasti ICT a kybernetické bezpečnosti spočívají taktéž v tom, do jaké míry je u konkrétního typu veřejné zakázky nezbytné, aby zadávací dokumentace pro potřeby podání nabídky obsahovala detailní technický popis stávajícího prostředí zadavatele nebo konkrétních bezpečnostních opatření. Tato problematika vykazuje značnou variabilitu, jelikož pro účely zachování dostatečné míry hospodářské soutěže

- je v některých případech postačující, aby zadavatel vymezil funkční, výkonové a bezpečnostní cíle, kterých má být plněním dosaženo, aniž by odhaloval interní detaily svého řešení,
- v jiných případech stačí uvést pouze obecný výčet stávajících technologií, s tím, že bude dostačující, když se s detailními parametry stávajícího prostředí vybraný dodavatel seznámí až v rámci předimplementační analýzy po uzavření smlouvy,
- a vyskytují se i případy, kdy je zadavatel nucen pro potřeby rozvoje informačního systému do zadávací dokumentace uvést kompletní popisy stávajícího systému včetně syntaxe jeho rozhraní, a tyto informace jsou zcela klíčové pro sestavení a podání nabídky.

Již ve fázi přípravy zadávací dokumentace by proto měl zadavatel zvážit, které informace jsou skutečně nezbytné pro pochopení předmětu plnění a které je vhodné poskytnout pouze v obecnější nebo agregované podobě, případně je neposkytovat vůbec.

Ochrana důvěrných informací se významně uplatní také v rámci předběžných tržních konzultací. Ty jsou v oblasti ICT a kybernetické bezpečnosti často užitečným nástrojem pro ověření proveditelnosti požadavků a zmapování trhu, současně však mohou představovat zvýšené riziko z pohledu bezpečnosti informací. Zadavatel by měl i v tomto případě poskytovat pouze takové informace, které jsou nezbytné pro dosažení cíle konzultace, a přijmout přiměřená opatření k ochraně jejich důvěrnosti. Součástí těchto opatření může být i závazek mlčenlivosti ze strany účastníků konzultace, avšak ani ten nenahrazuje povinnost zadavatele zvážit, zda je sdělení konkrétní informace v dané fázi skutečně nezbytné.

Rozdílné nároky na ochranu důvěrných informací se uplatní v závislosti na zvoleném druhu zadávacího řízení. V řízeních bez jednacího prvku je třeba vycházet z toho, že zadávací dokumentace a vysvětlení zadávací dokumentace jsou zpravidla přístupné neomezenému okruhu dodavatelů. Zadavatel by proto měl postupovat obezřetně při poskytování detailních technických a bezpečnostních informací a upřednostňovat formulaci požadavků na předmět veřejné zakázky prostřednictvím funkčních a výkonových parametrů. Zvláštní pozornost je třeba věnovat vysvětlením zadávací dokumentace v reakci na dotazy dodavatelů, neboť i jejich prostřednictvím může dojít k neúmyslnému zpřístupnění citlivých informací.

Naopak zadávací řízení s jednacím prvkem poskytují zadavateli větší flexibilitu v nakládání s důvěrnými informacemi. Umožňují poskytovat citlivé informace postupně, v návaznosti na jednotlivé fáze řízení, a pouze omezenému okruhu účastníků. Z hlediska kybernetické bezpečnosti může být tento postup vhodný zejména v případech, kdy je nezbytné sdělit detailnější informace o prostředí zadavatele, výsledcích analýzy rizik nebo konkrétních bezpečnostních opatřeních. I v těchto případech je však zadavatel povinen dbát na zachování rovného zacházení mezi účastníky v rámci dané fáze řízení a zajistit, aby žádný z nich nebyl neoprávněně zvýhodněn.

2.4.3 Nástroje ochrany důvěrných informací podle ZZVZ

Základní institut sloužící k ochraně důvěrné povahy informací je obsažen v § 36 odst. 8 ZZVZ, podle něhož může zadavatel požadovat, aby dodavatel přijal přiměřená opatření k ochraně informací důvěrné povahy, které mu zadavatel poskytuje nebo zpřístupňuje v průběhu zadávacího řízení. Toto ustanovení je formulováno obecně a nestanoví výčet konkrétních opatření, přičemž jejich volba a rozsah jsou ponechány na uvážení zadavatele s ohledem na povahu chráněných informací a zásadu přiměřenosti.

Ochranu důvěrných informací v průběhu zadávacího řízení lze zajišťovat zejména prostřednictvím:

- požadavků na přijetí přiměřených technických a organizačních opatření podle § 36 odst. 8 ZZVZ,
- smluvního zajištění mlčenlivosti podle § 36 odst. 8 ZZVZ,
- omezení zveřejnění části zadávací dokumentace na profilu zadavatele podle § 96 odst. 2 ZZVZ,
- využití výjimky z povinné elektronické komunikace podle § 211 odst. 5 písm. d) ZZVZ.

Důležitým nástrojem ochrany důvěrných informací je **smluvní zajištění mlčenlivosti**. Taková ochrana důvěrnosti standardně probíhá prostřednictvím požadavku zadavatele na uzavření samostatné dohody o mlčenlivosti s dodavateli. Jedná se o další doplněk k odpovědnému nakládání s informacemi. Povinnost chránit informace se následně promítá i do smlouvy na plnění veřejné zakázky, kde by měla být upravena nejen povinnost mlčenlivosti, ale i další bezpečnostní povinnosti dodavatele a případné sankce za jejich porušení.

Další možností ochrany důvěrných informací je vyhrazení práva zpřístupnit určité informace pouze přímo u zadavatele. V takovém případě může být ta část zadávací dokumentace, která obsahuje důvěrné informace, zpřístupněna dodavatelům pouze v místě určeném zadavatelem v tzv. reading-room (fyzický nebo virtuální prostor s logováním přístupů). Zadavatel může současně požadovat identifikaci osob, které se s těmito informacemi seznamují, a stanovit zákaz kopírování či pořizování záznamů těch částí dokumentace, jejichž zveřejnění by mu mohlo způsobit újmu, jakož i další opatření směřující k zamezení šíření důvěrných informací, vždy při zachování zásady rovného zacházení a přiměřenosti.

Zadavatel je povinen chránit nejen své vlastní důvěrné informace, ale také důvěrné informace dodavatelů, zejména obchodní tajemství a know-how obsažené v nabídkách. ZZVZ umožňuje dodavatelům označit části nabídky jako důvěrné ve smyslu § 218 odst. 1 ZZVZ, přičemž zadavatel je povinen takové označení respektovat, jsou-li splněny zákonné podmínky, a postupovat dle § 218 odst. 2 ZZVZ a souvisejících ustanovení. Současně však platí, že označení informace za důvěrnou nemůže bránit uplatnění práv na přezkum zadávacího řízení ani znemožnit kontrolu postupu zadavatele.

2.4.4 Zvláštní režimy a vazba na ZKB

Z pohledu ZKB představuje ochrana důvěrných informací v zadávacím řízení přirozenou součást řízení rizik a řízení dodavatelů. Zadavatelé, kteří jsou povinnými osobami podle ZKB, by měli rizika spojená s poskytováním informací v průběhu zadávacího řízení identifikovat a zohlednit v rámci svého systému řízení kybernetické bezpečnosti. Postupy zadávání veřejných zakázek by tak měly být v souladu s interní bezpečnostní dokumentací a zvolenými bezpečnostními opatřeními. Ochrana důvěrných informací v zadávacím řízení proto není pouze procesní otázkou veřejného zadávání, ale nedílnou součástí celkového přístupu organizace k zajištění kybernetické a informační bezpečnosti.

Pokud má být institut ochrany důvěrných informací aplikován ve vztahu k zadávací dokumentaci nebo jiným dokumentům uveřejňovaným v průběhu zadávacího řízení, které jsou způsobilé ovlivnit jeho výsledek, měl by být vykládán nikoli jako možnost informace neposkytnout, ale jako povinnost nalézt takové řešení, které zajistí ochranu citlivých informací a současně umožní co nejširší hospodářskou soutěž, například prostřednictvím postupů podle § 36 odst. 8 a § 96 odst. 2 ZZVZ.

V této souvislosti je třeba upozornit na § 96 odst. 2 ZZVZ, který umožňuje v návaznosti na opatření podle § 36 odst. 8 ZZVZ omezit zveřejnění příslušné části zadávací dokumentace na profilu zadavatele, a na § 211 odst. 5 písm. d) ZZVZ, který z důvodu ochrany informací zvláště citlivé povahy umožňuje výjimku z povinné elektronické komunikace mezi zadavatelem a dodavateli, pokud nelze dosáhnout rozumné úrovně zabezpečení prostřednictvím běžně dostupných komunikačních nástrojů.

V případě, že předmětem veřejné zakázky jsou utajované informace, je možné vůči osobě vybraného dodavatele využít postupu podle § 104 písm. c) ZZVZ, případně zadat veřejnou zakázku v režimu výjimky podle § 29 písm. b) ZZVZ, jsou-li naplněný zákonné předpoklady.

2.5 Kvalifikace dodavatelů a některé důvody pro jejich vyloučení

Bezpečnostní opatření přijímaná zadavatelem se mohou týkat nejen samotného předmětu plnění (technických podmínek či smluvních povinností), ale i osoby dodavatele a jeho způsobilosti být účastníkem zadávacího řízení. ZZVZ rozlišuje základní způsobilost, profesní způsobilost, ekonomickou kvalifikaci a technickou kvalifikaci. Kromě povinnosti požadovat prokázání základní způsobilosti dle § 74 ZZVZ a předložit výpis z obchodního rejstříku (či jiné obdobné evidence dle § 77 odst. 1 ZZVZ), záleží výlučně na zadavateli, zda a v jakém rozsahu bude s ohledem na předmět veřejné zakázky a okolnosti jejího zadávání požadovat prokázání dalších kritérií kvalifikace, tj. profesní způsobilosti, ekonomické či technické kvalifikace.

Zadavatel, který provádí hodnocení rizik jako vstupní předpoklad pro přijetí navazujících bezpečnostních opatření, by měl výsledky promítnout také do nastavení požadavků na kvalifikaci tak, aby došlo k minimalizaci expozice hrozbám plynoucím z rizikového profilu dodavatelů (účastníků zadávacího řízení) a ideálně k omezení (event. vyloučení) rizikových dodavatelů a jejich dodávek. Tato „risk-based logika“ je pro přípravu zadávacích podmínek zvlášť důležitá, protože dodavatelé se často dostávají do styku s citlivými informacemi zadavatele a s ohledem na charakter organizací často existuje veřejný zájem na ochraně dat.

V praxi se může tato logika promítnout například do požadavků na:

- doložení zkušeností s řešením bezpečnostních incidentů nebo provozem bezpečnostních opatření v obdobném prostředí,
- zavedené procesy řízení bezpečnosti informací a dodavatelského řetězce,
- prokázání existence bezpečnostních politik a postupů (např. řízení přístupů, řízení zranitelností nebo incident response).

Kvalifikaci lze požadovat pouze v oblastech stanovených ZZVZ (§ 73 a násl. ZZVZ), její rozsah však může zadavatel přizpůsobit objektivním potřebám a identifikovaným rizikům. Vhodně nastavené kvalifikační požadavky (tedy v souladu s § 36 odst. 1 a § 6 ZZVZ) tak představují legitimní nástroj pro omezení okruhu potenciálních dodavatelů odpovídající povaze a rizikovosti plnění.

*V souvislosti se stanovováním požadavků na prokázání kvalifikace, zejména pak technické kvalifikace, existuje bohatá judikatura. Základní premisa, na které relevantní judikatura stojí hovoří o tom, že **požadavky zadavatele nesmí být bezdůvodné, diskriminační a musí vycházet z objektivně zdůvodnitelných skutečností a korespondovat s účelem, kterého má být realizací veřejné zakázky dosaženo**. V tomto ohledu srov. např. rozsudek Nejvyššího správního soudu ze dne 11. 2. 2013, č. j. 7 As 7/2016-44, rozsudek Krajského soudu v Brně ze dne 19. 12. 2016, č. j. 31 Af 3/2015-29, nebo rozhodnutí předsedy ÚOHS ze dne 20. 10. 2016, č. j. ÚOHS-S0599/2016/VZ-42820/2016/551/OPa). Dále je v kontextu relevantní judikatury třeba reflektovat i situaci na daném trhu, a to ve smyslu, jaký budou mít jednotlivé požadavky na něj dopad. Krajský soudu v Brně v rozsudku ze dne 25. 9. 2023, č. j. 30 Af 77/2021-216, uvedl mj., že samotný fakt, že zadavatel zvolí zadávací podmínky, které zákon výslovně upravuje, a nepřekročí omezení, která jsou v příslušných ustanoveních obsažena, ještě nezaručuje, že zadávací dokumentace bude v souladu se zákonem o zadávání veřejných zakázek jako celkem (zejména s jeho § 36 odst. 1 ZZVZ).*

Zatímco požadavky ZZVZ na základní a profesní způsobilost jsou dány relativně pevně, v rámci ekonomické a technické kvalifikace lze požadavky stanovit dle legitimních potřeb zadavatele. Výstup z hodnocení rizik může odůvodnit zacílení na příslušnou úroveň ekonomické kvalifikace zejména tehdy, pokud zadavatel potřebuje ekonomicky stabilního a odolného partnera s ohledem na dlouhodobost smluvního vztahu.

Výstupy hodnocení rizik v dodavatelské oblasti se mohou promítnout do parametrického nastavení technické kvalifikace dodavatelů, zejména se jedná o možnosti využití:

- **požadavků na zkušenosti dodavatele** dle § 79 odst. 2 písm. b) ZZVZ (tj. toho, co bude považováno za významné dodávky nebo služby),
- **odbornosti realizačního týmu** dle § 79 odst. 2 písm. c) a d) ZZVZ (zejména zkušenosti, specifická praxe, relevantní certifikace pracovníků v různých rolích),
- **procesů řízení bezpečnosti** informací v organizaci dodavatele dle § 79 odst. 2 písm. e) a § 80 odst. 1 ZZVZ (vč. požadavku na doložení certifikátu ISO řady 27000),
- **přehledu o řízení dodavatelského řetězce a systémů sledování dodavatelského řetězce**, které dodavatel bude moci uplatnit při plnění veřejné zakázky dle § 79 odst. 2 písm. F) ZZVZ,
- **testování (zkoušek vzorků) nabízeného plnění** dle § 79 odst. 2 písm. k) ZZVZ (například možnost prezentace funkčního jádra informačního systému za účelem ověření, zda zadavatelem požadované funkce a vlastnosti jsou naplněny).

Pro oblast referenčních požadavků obecně platí, že reference by měly vyjadřovat reálnou zkušenostní hodnotu, která je nezbytná pro kvalitní plnění zadávané veřejné zakázky. Jednotlivé reference by neměly kumulovat příliš mnoho parametrů, jelikož úměrně s rostoucí složitostí reference klesá pravděpodobnost jejího výskytu na trhu a současně klesá pravděpodobnost přítomnosti reálné přidané zkušenostní hodnoty, která z reference vyplývá. Pokud tedy např. zadavatel požaduje, aby měl dodavatel zkušenosti s řešením MFA (multi-factor authentication) a dodávkou systému pro analýzu síťového provozu, pak bude pravděpodobně dostačující, pokud

dodavatelé prokážou tyto zkušenosti dvěma samostatnými referencemi, zatímco povinný konglomerát obou aktivit v jedné referenci může být spíše otázkou náhodného výskytu na trhu, bez speciální přidané zkušenostní hodnoty. Vždy je však nutné zohlednit veškeré aspekty konkrétní situace.

Pro oblast veřejných zakázek v ICT a kybernetické bezpečnosti je typické, že k prokázání odbornosti jednotlivých členů realizačního týmu dodavatele může zadavatel požadovat doložení nejrůznějších **soukromoprávních certifikátů**, např. v oblasti architektury kybernetické bezpečnosti, risk managementu, penetračního testování, projektového řízení (tzv. vendor neutrální certifikáty, jelikož nejsou vázány na konkrétní zařízení či program), anebo řadu různých vendor-specifických certifikací pro ovládání zařízení a programů, které již zadavatel provozuje (např. Cisco, Microsoft apod.). Požadavky na certifikaci musí být stanoveny přiměřeně a zadavatel musí vždy umožnit prokázání certifikace alternativními či vyššími certifikacemi, které prokazují stejné dovednosti. Není-li to odůvodněno specifiky veřejné zakázky, není rovněž vhodné kumulovat požadavky na disponování dvěma či více různými certifikacemi současně u konkrétního člena týmu (namísto připuštění možnosti prokázat tyto certifikace u dvou různých osob), jelikož se tím razantně snižuje pravděpodobnost výskytu takové osoby na trhu (pro odůvodnění takového požadavku by zadavatel musel nalézt reálnou přidanou hodnotu). V řadě případů je rovněž reálné certifikát substituovat prokázáním specifické praxe či zkušeností s konkrétními projekty.

> *Tzv. vendor-specifické certifikáty je zadavatel oprávněn požadovat v rámci technické kvalifikace pouze v případě, že příslušná technologie, na níž certifikace navazuje, je integrální součástí stávajícího prostředí zadavatele a technické řešení definované technickými podmínkami na tuto technologii bezprostředně navazuje, existuje tedy současně i odůvodnění dle § 89 odst. 5 ZZVZ.*

Požadovaná certifikace se může týkat i samotného dodavatele jako právnické osoby, a to zejména v podobě doložení managementu bezpečnosti informací v organizaci. Je-li zadavatelem doložena souvislost s kvalitou poskytovaného plnění, tj. existuje-li odůvodnění předmětem plnění veřejné zakázky, lze po účastnících zadávacího řízení požadovat doložení platné certifikace dokládající splnění bezpečnostních požadavků, např. certifikát ISO řady 27000 (viz rozsudek Nejvyššího správního soudu ze dne 25. 9. 2019, č. j. 6 As 113/2019-32).

Požadavky založené na normách ohledně zajištění systému řízení bezpečnosti informací se budou v mnoha případech krýt s požadavky na naplnění kritérií určených v ZKB. Plnění povinností stanovených povinným osobám v ZKB, potažmo jeho prováděcími právním předpisy, pak z povahy věci není považováno za neodůvodněné omezování hospodářské soutěže (blíže viz kapitola 1.2 této metodiky).

Ve věci testování (zkoušek vzorků) nabízeného plnění musí zadavatel s ohledem na dodržení zásady transparentnosti uchovat záznamy a dokumenty i o těchto zkouškách a prezentacích (např. videozáznam z prezentace, fotodokumentace zkoušky vzorku a protokol o zkoušce apod.), a všechny tyto záznamy archivovat v souladu s § 216 ZZVZ.

Zadavatel je přitom povinen vyloučit ze zadávacího řízení dodavatele, který má být vybrán k plnění veřejné zakázky, jehož nabídka nesplňuje zadávací podmínky, tedy včetně podmínek kvalifikace (§ 48 odst. 8 ZZVZ).

Zvláštním oprávněním, které zadavatel v rámci posouzení nabídky má, je možnost vyloučit účastníka zadávacího řízení, pokud zadavatel prokáže, že dodavatel má protichůdné zájmy. Dle § 79 odst. 1 druhé věty ZZVZ platí, že zadavatel může považovat technickou kvalifikaci za neprokázanou, pokud prokáže, že dodavatel má protichůdné zájmy, které by mohly negativně ovlivnit plnění veřejné zakázky (i přesto, že takový dodavatel řádně prokázal splnění kritérií technické kvalifikace doložením všech požadovaných údajů a dokladů). Aby bylo možné dodavatele vyloučit postupem dle § 48 odst. 2 písm. a) ZZVZ (v případě vybraného dodavatele dle § 48 odst. 8 ZZVZ), zadavatel bude muset být nejen schopen prokázat existenci protichůdných zájmů dodavatele (například hospodářských), ale současně i to, že tyto zájmy jsou způsobilé (alespoň potenciálně) negativně ovlivnit plnění veřejné zakázky. Na takového dodavatele by se z hlediska vyloučení hledělo, jako by splnění kritérií technické kvalifikace v plném rozsahu neprokázal.

Jiným specifickým případem je možnost vyloučení účastníka zadávacího řízení, který se dopustil závažného profesního pochybení, které zpochybňuje jeho důvěryhodnost (§ 48 odst. 5 písm. f) ZZVZ), anebo závažných nebo dlouhodobých pochybení při plnění dřívějšího smluvního vztahu se zadavatelem zadávané veřejné zakázky, nebo s jiným veřejným zadavatelem, která vedla k vzniku škody, předčasnému ukončení smluvního vztahu nebo jiným srovnatelným sankcím (§ 48 odst. 5 písm. d) ZZVZ). Je zde potřeba zdůraznit, že zadavatel musí takovou skutečnost prokázat, což může být v praxi značně obtížné. ZZVZ ale zadavatele nijak neomezuje ve způsobu zjišťování použitelných informací, záleží proto na zadavateli, jaké zdroje pro zjišťování informací využije (lze např. uvažovat o kontaktování známých příjemců služeb či dodávek účastníka zadávacího řízení). I přes naznačené praktické komplikace je z hlediska kybernetické bezpečnosti žádoucí, aby tyto možnosti vyloučení dodavatele pro nezpůsobilost zadavatel zvážil, a to zejména v případech existence vážných a podložených důvodů.

Vybraný dodavatel může být vyloučen rovněž na základě ustanovení § 122 odst. 8 ZZVZ, pokud nebylo možné zjistit údaje o jeho skutečném majiteli z evidence skutečných majitelů, nebo pokud zahraniční vybraný dodavatel údaje o svém skutečném majiteli dle § 122 odst. 6 nepředložil.

Rizika spojená s dodavatelem mohou být také odvozována od země jeho původu, resp. geopolitické dimenze. Analýza rizik zadavatele může ve zvláštních případech identifikovat riziko zneužití státní moci pro přístup k aktivům, mj. v souvislosti s vývojem geopolitické situace; jako hrozba mohou být vnímáni dodavatelé napojení na jurisdikce, jejichž legislativa umožňuje zásah zpravodajských služeb a silových složek do důvěrnosti, dostupnosti, integrity uchovávaných nebo zpracovávaných dat. Pokud zadavatel zvažuje protiopatření, vedle kvalifikačních požadavků mohou k omezení či nepřipuštění účasti rizikového dodavatele vést i kroky založené na odmítnutí účasti dodavatelů či výrobků ze třetích zemí (blíže viz kapitola 3 této metodiky).

Z rozhodnutí ÚOHS ze dne 22. 12. 2020, č. j. ÚOHS-41587/2020/510/MKo plyne, že pokud se zadavatel rozhodne účastníka zadávacího řízení vyloučit na základě ustanovení § 48 odst. 5 písm. d) ZZVZ důkazní břemeno ohledně prokázání naplnění výše uvedených podmínek leží právě na něm. Zadavatel musí naplnění všech vzájemně souvisejících zákonných podmínek vyplývajících z předmětného ustanovení ZZVZ prokázat a odůvodnit. Zadavatel tedy musí prokázat, že se účastník dopustil více než jednoho pochybení, že k uvedeným pochybením došlo při plnění dřívějšího smluvního vztahu se zadavatelem zadávané veřejné zakázky nebo při plnění dřívějšího smluvního vztahu s jiným veřejným zadavatelem, že se uvedených pochybení účastník dopustil v posledních 3 letech od zahájení zadávacího řízení, že se jednalo o pochybení závažná nebo dlouhodobá a že tato pochybení vedla ke vzniku škody, předčasnému ukončení smluvního vztahu nebo k jiným srovnatelným sankcím.

Podle rozhodnutí předsedy ÚOHS ze dne 25. 7. 2019, sp. zn. R0093/2019/VZ, č. j. ÚOHS-R0093/2019/VZ-20435/2019/321/OMa, je třeba za srovnatelné sankce považovat veškeré právní prostředky, které právní řád či ujednání stran poskytuje zadavateli k tomu, aby zhojil následky pochybení dodavatele či aby jej za toto pochybení sankcionoval. Typicky se bude jednat o práva z vadného plnění či právo na smluvní pokutu. Z rozhodnutí předsedy Úřadu pro ochranu hospodářské soutěže ze dne 12. 12. 2019, sp. zn. S0376/2019/VZ, č. j. ÚOHS-S0376/2019/VZ-34408/2019/522/NRi, dále plyne, že vyloučení účastníka řízení je pro zadavatele snazší, pokud ÚOHS o pochybení účastníka již v minulosti rozhodl (možnost odkázat na rozhodnutí, ale vždy je třeba znovu odůvodňovat splnění časové podmínky).

2.6 Omezení poddodávek

Vzhledem k povaze informačních a komunikačních systémů může být poskytování dodávek ICT prostřednictvím poddodavatelů rizikem, které musí poskytovatel regulované služby řídit, popřípadě by jej v některých případech neměl připustit. Poddodavatelé mohou být považováni za potenciální riziko, zejména pokud jde o dodavatele produktů ze zemí mimo EU či pokud zadavatel v konkrétním případě vyhodnotí jiné bezpečnostní hrozby s určitými poddodávkami.

Mezi typická rizika spojená s poddodavateli mohou patřit zejména:

- riziko neoprávněného přístupu k primárním nebo podpůrným aktivům (např. v rámci vzdálené správy),
- riziko přenosu nebo ukládání dat mimo kontrolované prostředí zadavatele,
- riziko nedostatečné kontroly nad dodavatelským řetězcem (např. vícestupňové poddodávky),
- rizika vyplývající z právního a bezpečnostního prostředí, ve kterém poddodavatel působí.

Konkrétní identifikace těchto rizik by měla vždy vycházet z analýzy rizik zadavatele.

Jakkoli je výchozí tezí ZZVZ, že absolutní zákaz poddodávek není přípustný, zadavatel může v rámci hodnocení rizik a při přípravě zadávacích podmínek využít celého instrumentária zákonných institutů ke zohlednění svých legitimních potřeb. Pro vymezení pravidel poddodávek má zejména následující nástroje:

2.6.1 Způsobilost poddodavatelů a požadavek na jejich nahrazení

Zadavatel může požadovat doklady prokazující základní a profesní způsobilost poddodavatelů dle § 85 odst. 1 ZZVZ a podle § 85 odst. 2 ZZVZ může požadovat nahrazení poddodavatele, který neprokáže splnění požadovaných kritérií způsobilosti nebo je nezpůsobilý.

2.6.2 Transparentnost dodavatelského řetězce už v nabídce a identifikace poddodavatelů

Zadavatel je oprávněn v zadávací dokumentaci požadovat, aby účastník zadávacího řízení již v nabídce určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů (§ 105 odst. 1 písm. a) ZZVZ), resp. aby předložil seznam poddodavatelů a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit (§ 105 odst. 1 písm. b) ZZVZ).

Specifickým případem je možnost zadavatele požadovat doložení autorizovaného partnerství poddodavatele s výrobcem zařízení, pokud má zajišťovat podporu dodaných řešení, včetně např. logistiky náhradních dílů.

2.6.3 Vyhrazení významných činností jen hlavnímu dodavateli

Omezení plnění zakázky poddodavateli je možné dle § 105 odst. 2 ZZVZ u veřejné zakázky na stavební práce, na služby nebo případně u veřejné zakázky na dodávky zahrnující umístění, implementaci nebo montáž. Zadavatel v zadávací dokumentaci určí významné činnosti, u nichž požaduje, aby byly plněny přímo vybraným dodavatelem (tedy s vyloučením plnění poddodavatele).

> *K vymezení „významné činnosti" dle § 105 odst. 2 ZZVZ jakožto neurčitého právního pojmu je možno odkázat na rozsudky Nejvyššího správního soudu ze dne 12. 11. 2024, č. j. 10 As 122/2024-60, a ze dne 23. 8. 2024, č. j. 5 As 258/2022-61, z nichž vyplývá,* ***že možnost vyloučit použití poddodavatele podle § 105 odst. 2 ZZVZ je omezena pouze na činnosti natolik významné, že je nemůže plnit jakýkoliv dodavatel v oboru, ale pouze vysoce kvalifikovaní a specializovaní odborníci****. Účelem výhrady je získat zvýšenou kontrolu a dohled nad zásadními částmi plnění.*

Významné činnosti by měly být vymezeny konkrétně a jednoznačně (nikoli obecně), a to ideálně v návaznosti na výsledky analýzy rizik zadavatele. Typicky se může jednat o činnosti spojené s přístupem ke kritickým částem infrastruktury, správou identit a přístupových oprávnění nebo nakládáním s citlivými daty.

Je přitom vhodné zdůraznit, že rozsah významné části zakázky není v ZZVZ explicitně stanoven a zákon tak dává zadavateli možnost takto určit značnou část zakázky; v takovém případě je velmi důležité mít toto určení rozumně odůvodněno pro případný přezkum. Využití tohoto oprávnění z bezpečnostních důvodů je bezpochyby možné.

V této souvislosti lze poukázat např. na rozhodnutí předsedy ÚOHS sp. zn. R0164/2024/VZ, č. j. ÚOHS-47271/2024/161 ze dne 11. 12. 2024, dle něhož ***výhrada plnění vybraným dodavatelem musí v zásadě splňovat dvě podmínky: musí být vymezena konkrétním a věcným způsobem a musí obstát z hlediska základních zásad zadávání****, tedy zde zejm. z hlediska zákazu neodůvodněného omezování okruhu dodavatelů. Pokud zadavatel vymezil vybrané činnosti věcně široce tak, že jsou jimi prakticky všechny činnosti, které tvoří podstatu plnění, není taková výhrada v rozporu se zákonem, má-li pro ni zadavatel relevantní důvody.*

2.6.4 Omezení řetězení a úrovní poddodávek

Z bezpečnostního posouzení (analýzy rizik) může vyplynout, že by nemělo docházet k řetězení dodávek různých poddodavatelů; omezení poddodávek v určitém rozsahu předmětu plnění nebo např. omezení na jednu přípustnou poddodavatelskou úroveň může zadavatel vhodně promítnout i do podmínek kvalifikace.

V praxi může zadavatel tato omezení formulovat zejména:

- stanovením maximální přípustné úrovně poddodavatelského řetězce (např. zákaz dalšího poddodavatelství nad rámec jedné úrovně),
- vyhrazením vybraných činností, které nesmí být plněny prostřednictvím poddodavatelů,
- požadavkem na identifikaci poddodavatelů již v nabídce, včetně vymezení jejich role,
- stanovením povinnosti získat předchozí souhlas zadavatele se zapojením dalšího poddodavatele v průběhu plnění.

Tato omezení by měla vycházet z analýzy rizik zadavatele a být přiměřená povaze plnění. Typicky mohou být odůvodněna zejména v případech, kdy by řetězení poddodavatelů vedlo ke ztrátě kontroly nad přístupem k citlivým datům, nad řízením bezpečnostních opatření nebo nad dodavatelským řetězcem jako takovým.

2.6.5 Dohled nad poddodavateli z důvodu mezinárodních sankcí

Zadavatel nezadá veřejnou zakázku účastníkovi zadávacího řízení, pokud je to v rozporu s mezinárodními sankcemi podle zákona upravujícího provádění mezinárodních sankcí (více v kapitole 3.2); takového účastníka zadavatel vyloučí dle § 48a odst. 1 ZZVZ. Tato povinnost může být iniciována i v situaci, kdy mezinárodní sankce dopadá pouze na poddodavatele účastníka.

Současně platí, že mimo vyhrazené významné činnosti může být seznam poddodavatelů měněn, a to i za účelem vyhnutí se povinnosti vyloučit účastníka v důsledku rozporu s mezinárodními sankcemi. K získání úplného přehledu o poddodavatelích zapojených do plnění veřejné zakázky může dojít až v průběhu plnění zakázky skrze institut upravený v § 105 odst. 3, resp. odst. 4 ZZVZ. Využití této možnosti by mělo být uvedeno v zadávací dokumentaci.

2.6.6 Smluvní řízení poddodavatelů

Zásadní je také úprava vztahů zadavatele, dodavatele a poddodavatelů ve smlouvě na plnění veřejné zakázky, která by měla přesně stanovit, jak budou probíhat práce s poddodavateli, jak bude probíhat komunikace s nimi a kontrola. Smlouva by také měla obsahovat efektivní sankční ustanovení pro případ porušení povinností. Zadavatel, zejména pokud se jedná o poskytovatele regulované služby v režimu vyšších povinností, je povinen řídit své dodavatele v rozsahu § 9 vyhlášky o bezpečnostních opatřeních. Podle přílohy č. 5 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností je třeba jako obsahovou náležitost smlouvy s dodavatelem zvážit 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.

2.7 Kritéria hodnocení nabídek

Hodnocení nabídek je klíčovou fází zadávacího řízení, v níž zadavatel vybírá ekonomicky nejvýhodnější nabídku a fakticky rozhoduje o tom, kdo bude plnit veřejnou zakázku. Ekonomická výhodnost je zároveň jediným „společným jmenovatelem“, podle něhož musí být nabídky v řízení vzájemně poměřovány – ať už jen podle ceny, nebo podle kombinace ceny a kvality. V ICT (kybernetické bezpečnosti) je přitom kvalita úzce spojená s bezpečností. Nedostatečná kvalita plnění představuje významné riziko pro ochranu klíčových systémů a dat zadavatele, a proto je legitimní, aby zadavatel bezpečnost (a související kvalitativní prvky) promítl i do hodnocení.

> *V případě vícekriteriálního hodnocení je třeba pamatovat na to, zda při jeho nastavení nedochází de facto k omezení soutěže a kritérium hodnocení se tak nestává další (skrytou) technickou podmínkou. V této souvislosti lze odkázat na rozhodnutí předsedy ÚOHS zde dne 24. 6. 2025, sp. zn. R0051/2025/VZ, č. j. ÚOHS-22941/2025/163. V daném případě v důsledku nastavení kritérií kvality a jejich vah došlo k situaci, kdy se sice mohlo do zadávacího řízení veřejné zakázky formálně přihlásit více dodavatelů, v rámci hodnocení by však s výjimkou jednoho získali ostatní dodavatelé minimální bodový zisk (bez možnosti kompenzace této ztráty absurdně nízkou a netržní cenou). Při takovémto způsobu nastavení kritérií hodnocení je ze strany dozorového orgánu na tato kritéria nahlíženo výrazně přísněji z hlediska toho, jak je zadavatel musí případně odůvodnit, jelikož reálně představují „tvrdou“ překážku pro možnost účasti dodavatele v zadávacím řízení.*

V praxi zadavatelé v případě ICT zakázek často volí hodnocení nabídek pouze podle nejnižší nabídkové ceny, mj. z důvodu obav ze složitosti multikriteriálního hodnocení. Tento přístup je však dvojsečný: procesní jednoduchost může negativně dopadnout na kvalitu a bezpečnost výsledného plnění (nejlevnější nebývá nejlepší) a riziko se může projevit až v provozu.

Použití nejnižší ceny jako jediného kritéria je legální způsob hodnocení nabídek v oblasti ICT a kybernetické bezpečnosti (hodnocení nabídek výhradně na základě nejnižší nabídkové ceny je vyloučeno pouze u některých druhů zadávacích řízení a u některých typů služeb, do kterých ale plnění

v oblasti ICT a kybernetické bezpečnosti nespadají). O vhodný způsob se typicky bude jednat tehdy, když:

- zadavatel má velmi kvalitně a přesně nastavené závazné požadavky v zadávacích podmínkách (technické, bezpečnostní, obchodní požadavky), a
- nepotřebuje získat přidanou hodnotu nad rámec minimálních parametrů (např. vyšší dostupnost, či rozšířené funkcionality, než sám předepsal).

Pokud má zadavatel důvod požadovat vyšší úroveň zabezpečení, robustnější provozní model, kvalitnější služby podpory nebo vyšší jistotu funkčnosti (například u kritických systémů), je namístě volit ekonomickou výhodnost podle kvality a stanovit dílčí kvalitativní kritéria ve smyslu § 116 ZZVZ. Naopak pro běžný ICT nákup či pořízení standardizovaných bezpečnostních řešení, pokud zadavatel nepožaduje nadstandardní parametry, lze zvolit hodnocení nabídek podle nabídkové ceny, příp. podle nákladů životního cyklu.

S ohledem na flexibilitu ZZVZ je tedy možné, aby bezpečnostní úroveň nabízeného plnění byla stanovena jako součást kritérií kvality; v takovém případě nedochází k apriornímu vyloučení technologií, ale k porovnání relevantních nabídek tak, aby objektivně bezpečnější řešení bylo lépe hodnoceno. Zadavatel však musí v zadávací dokumentaci popsat, na základě jakých skutečností a jakým způsobem bude bezpečnost hodnocena.

Kritéria kvality musí být nastavena tak, aby byly nabídky podle nich porovnatelné a naplnění kritérií ověřitelné. To platí zvlášť u bezpečnosti, kde hrozí riziko „marketingového“ popisu bez reálné hodnoty. Z hlediska přístupu lze doporučit, aby zadavatel vymezil bezpečnostní kritéria ve vazbě na:

- atributy bezpečnosti (důvěrnost, integrita, dostupnost),
- cílovou úroveň zabezpečení a důležitost aktiva,
- architekturu a prostředí, do něhož bude řešení implementováno.

Z praktického pohledu může bezpečnostní úroveň řešení jako kvalitativní kritérium spočívat v hodnocení nadstandardních funkcionalit zvyšujících bezpečnost (nad rámec minimálních parametrů stanovených zadavatelem), hodnocení bezpečnostních vlastností podložených objektivními a uznávanými testy/benchmarky nebo hodnocení reakce na modelové situace (např. postup řešení bezpečnostního incidentu). Dalšími kritérii kvality mohou být úroveň servisní a technické podpory (dostupnost podpory, způsob eskalace, garantované lhůty pro opravy bezpečnostních zranitelností apod.), zkušenosti klíčových osob podílejících se na plnění (např. architekta bezpečnosti), vyšší počet podporovaných integrací s technologiemi zadavatele (pokud je reálně zvýšena využitelnost řešení zadavatelem anebo sníženo provozní riziko) nebo náklady životního cyklu s provozní efektivitou (možnost hodnocení nároků na HW infrastrukturu, platformní služby a efektivity užívání systému, případně i prostřednictvím způsobu modelových situací). ZZVZ také umožňuje zadavateli pracovat se vzorky (funkčním řešením) a testováním deklarovaných funkcionalit v rámci hodnocení nabídek.

Je ovšem třeba zdůraznit, že kritéria hodnocení by neměla být vnímána jako náhrada minimálních bezpečnostních požadavků, když „bezpečnostní základnu“ musí zadavatel v zadávacích podmínkách a smlouvě na plnění veřejné zakázky jasně vymezit. Možnost hodnocení kvality a bezpečnosti řešení v nabídkách má sloužit k výběru lepších variant mezi bezpečnými řešeními. Je proto se třeba vyvarovat situaci, že by zadavatel ponechal zohlednění rizik až do fáze hodnocení, pokud by toto vedlo k tomu, že zadavatel by musel vybrat řešení, které nevyhoví jeho potřebám (včetně bezpečnostních).

2.8 Postupy před uzavřením smlouvy na plnění veřejné zakázky

Ustanovení § 104 ZZVZ vymezuje kategorii požadavků (tzv. dalších podmínek pro uzavření smlouvy), které se uplatní vůči osobě vybraného dodavatele před uzavřením smlouvy a které zadavatel může předem vymezit v zadávací dokumentaci. Tato fáze zadávacího řízení představuje poslední příležitost zadavatele ověřit, že vybraný dodavatel skutečně splňuje všechny požadavky stanovené v zadávacích podmínkách, a to ještě před tím, než je zadávací řízení dokončeno uzavřením smlouvy.

Nejde však o prostor pro doplňování nebo zpřísňování zadávacích podmínek ani pro „dohánění“ jejich nedostatečné přípravy. Zadavatel může v této fázi pouze ověřovat splnění požadavků, které byly předem transparentně stanoveny.

Tato fáze je významná zejména z hlediska eliminace rizik, která se v ICT/kybernetické bezpečnosti typicky projeví až v procesu realizace (např. v podobě nefunkčnosti řešení, nedostatečných bezpečnostních parametrů nebo rizikového dodavatelského řetězce apod.).

Současně je třeba respektovat základní pravidlo, že v zadávacích řízeních bez jednacího prvku po uplynutí lhůty pro podání nabídek již nelze připustit změny zadávacích podmínek ani obsahové změny nabídek. Proto musí všechny postupy, které chce zadavatel před uzavřením smlouvy uplatnit (testy, vzorky, dodatečné doklady, bezpečnostní prověření), vycházet z předem nastavených pravidel, která budou předvídatelně popsána v zadávací dokumentaci.

ZZVZ poskytuje zadavateli flexibilitu, aby rozhodl, že některé požadavky nemusí být doloženy přímo jako součást nabídky (ani pro účely prokázání kvalifikace či hodnocení nabídek), ale zadavatel je může požadovat až po celkovém vyhodnocení nabídek – tedy jen od vybraného dodavatele. To umožňuje, aby všemi bezpečnostními požadavky nebyli zatíženi všichni účastníci zadávacího řízení, ale zadavatel mohl soustředit své kapacity pouze na finalistu, a tím současně snížit riziko, že bude uzavřena smlouva na nefunkční nebo nedostatečně bezpečné řešení.

Z hlediska kybernetické bezpečnosti může jít v rámci zákaznického auditu např. o doložení:

- dalších certifikátů či auditních reportů (případně i u poddodavatelů), ověření původu dodavatele či jeho vlastnické struktury,
- potvrzení o autorizovaném partnerství vybraného dodavatele (nebo jeho poddodavatele) s výrobcem dodávaného plnění, vč. Garancí servisní podpory ze strany výrobce či autorizovaného servisního střediska,

- interních procesů relevantních pro bezpečnost (řízení zranitelností, incident response, úroveň dodržovaných bezpečnostních standardů),
- výsledků penetračních testů či bezpečnostních prověrek (případně i u poddodavatelů).

Klíčové je, aby šlo o podmínky předem transparentně stanovené; zadavatel tím nesmí fakticky měnit soutěžený předmět plnění, ani souvisejí zadávací podmínky, ale ověřuje splnění požadavků, které již předem stanovil jako nezbytné pro uzavření smlouvy.

V praxi lze významnou část úkonů před uzavřením smlouvy navázat na výzvu vybranému dodavateli dle § 122 odst. 3 ZZVZ.

2.8.1 Hodnocení rizik významného dodavatele

Pokud je z povahy veřejné zakázky zřejmé, že její plnění bude zajišťováno **významným dodavatelem** ve smyslu prováděcích právních předpisů k ZKB, vychází zadavatel z této skutečnosti již při přípravě zadávací dokumentace. Zadavatel v takovém případě předem zohlední požadavky vyplývající z řízení rizik a z právní úpravy kybernetické bezpečnosti a promítne je do zadávacích podmínek tak, aby bylo všem dodavatelům zřejmé, že plnění veřejné zakázky bude realizováno v režimu významného dodavatele.

Povinnost provést hodnocení rizik souvisejících s plněním významného dodavatele podle § 9 odst. 2 písm. a) vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností se ve veřejném sektoru typicky naplňuje prostřednictvím zadávacího řízení podle ZZVZ. Nejde přitom o samostatné nebo dodatečné hodnocení konkrétního vybraného dodavatele, ale o systematické promítnutí identifikovaných rizik do zadávacích podmínek, požadavků na dodavatele a smluvních ujednání, a o následné ověření jejich splnění.

V této fázi zadávacího řízení zadavatel zejména stanoví bezpečnostní, technické, organizační a smluvní požadavky odpovídající režimu významného dodavatele a vytvoří předvídatelný rámec pro jejich kontrolu. Dodavatelé tak již při podání nabídky vědí, že se ucházejí o plnění, u něhož se uplatní zvýšené požadavky na kybernetickou bezpečnost, a mohou tomu přizpůsobit své nabídky.

Ověření splnění těchto požadavků se následně uplatní zejména v rámci postupů podle § 104 ZZVZ a v návaznosti na výzvu vybranému dodavateli podle § 122 odst. 3 ZZVZ. Smyslem těchto postupů není měnit nebo zpřísňovat zadávací podmínky, ale ověřit, že vybraný dodavatel skutečně splňuje předem stanovené požadavky, které byly na základě řízení rizik vymezeny již v zadávací dokumentaci.

Skutečnost, že požadavky vyplývající z řízení rizik významného dodavatele byly promítnuty do zadávacích podmínek však nevylučuje, že v průběhu zadávacího řízení nebo po jeho skončení vyjdou najevo okolnosti, které znemožňují realizaci plnění v souladu s povinnostmi podle zákona o kybernetické bezpečnosti. Může se jednat například o nové skutečnosti týkající se dodavatelského řetězce, technického řešení nebo regulatorního rámce, které nebylo možné v době přípravy zadávací dokumentace předvídat.

V takovém případě může zadavatel dospět k závěru, že zadávací řízení nelze dokončit nebo že smluvní vztah nelze uzavřít či v něm pokračovat, pokud by jeho realizace vedla k porušení právních povinností zadavatele, resp. k nepřijatelnému ohrožení jeho kybernetické bezpečnosti. Zrušení zadávacího řízení, neuzavření smlouvy nebo ukončení smluvního vztahu však nepředstavuje důsledek samotného „hodnocení rizik významného dodavatele“, ale reakci na objektivní skutečnost, že plnění veřejné zakázky není možné uskutečnit v souladu s právními předpisy, tj. při zachování požadované úrovně kybernetické bezpečnosti. Jakýkoli takový postup musí být vždy proveden v souladu se ZZVZ, a tedy též řádně odůvodněn, aby byl přezkoumatelný. **Zadavatel musí být schopen doložit, že přijaté rozhodnutí vychází z objektivních a relevantních skutečností a že nevede k obcházení zásad transparentnosti, rovného zacházení a zákazu diskriminace.**

2.9 Obchodní/smluvní podmínky

2.9.1 Význam smlouvy v kontextu kybernetické bezpečnosti

Smlouva na předmět plnění veřejné zakázky v oblasti ICT a kybernetické bezpečnosti spolu s vlastním obsahem předmětu plnění jsou z hlediska kybernetické bezpečnosti klíčovými prvky, jejichž existence v rámci času přesahuje proces zadávacího řízení do budoucnosti. Bezpečnostní požadavky, které nejsou promítnuty do smluvních povinností dodavatele, budou zpravidla jen obtížně vymahatelné, resp. jejich následné upřesňování či doplňování ve smlouvě může být spojeno s dodatečnými náklady a obecně s posuzováním limitů přípustnosti změn závazku (k tomu blíže viz kapitola 2.10 této metodiky).

Proto má zadavatel již ve fázi přípravy zadávacích podmínek převést identifikovaná kybernetická rizika a požadovaná bezpečnostní opatření do konkrétních smluvních závazků, včetně mechanismů kontroly, nápravy, sankcí apod. Metodicky platí, že smluvní nastavení má být přiměřené rizikům, hodnotě a kritičnosti pořizovaného plnění, a má zároveň respektovat mantinely zadávání veřejných zakázek (zejména zásady dle § 6 ZZVZ). Současně platí, že požadavky, které by v běžné veřejné zakázce mohly případně působit restriktivně, mohou být za určitých okolností přiměřené, pokud jsou řádně odůvodněny povahou plnění a bezpečnostními riziky.

> *Dle rozhodnutí ÚOHS sp. zn. ÚOHS-R0048/2026/VZ, č. j. 15725/2026/161 ze dne 29. 4. 2026 v předmětné věci došlo na základě odůvodněných objektivních provozních a bezpečnostních důvodů a legitimních potřeb zadavatele, vyplývajících z charakteru infrastruktury, v níž bude veřejnou zakázkou poptávané zboží nasazeno, k určitému omezení hospodářské soutěže, avšak nikoliv na konkrétního výrobce, ale pouze na příslušnost dodavatele k oficiální distribuční síti kteréhokoliv relevantního výrobce. Omezení okruhu potenciálních dodavatelů samo o sobě nečiní zadávací podmínky nezákonnými, sledují-li legitimní cíl a odpovídají-li zásadě proporcionality. Tři sporné zadávací podmínky,* ***tj. požadavek originálního a nového zboží určeného pro evropský trh, požadavek autorizovaného partnerství a požadavek podpory servisního střediska, dodavatelům bezdůvodně přímo nebo nepřímo nezaručovaly konkurenční výhodu a ani nevytvářely bezdůvodné překážky hospodářské soutěže.***

Způsob pojetí obchodních podmínek není právní úpravou jednotně předepsán. Za obchodní podmínky dle § 37 odst. 1 písm. c) ZZVZ je třeba považovat jednotlivé požadavky zadavatele na obsah smlouvy na plnění veřejné zakázky, které zadavatel uvede v zadávací dokumentaci, i pokud nebudou mít podobu návrhu (vzoru) smlouvy. Smluvní nebo obchodní podmínky tedy mohou být vyjádřeny ve formě závazného návrhu smlouvy, který bude součástí zadávacích podmínek, či mohou být uvedeny jako jednotlivé obchodní a smluvní podmínky vyjmenované v zadávací dokumentaci.

Dle rozhodnutí ÚOHS sp. zn. S0242/2023/VZ, č. j. 29590/2023/500 ze dne 7. 8. 2023 smluvní podmínky představují specifickou část zadávací dokumentace. Zákon nestanoví, jaké smluvní podmínky mají být obsahem smlouvy uzavřené na realizaci předmětu plnění veřejné zakázky. Vymezení smluvních podmínek zákon ponechává na uvážení smluvních stran, kdy je zřejmé, že se zde primárně promítnou potřeby a požadavky zadavatele, neboť právě ten nejlépe ví, co potřebuje a za jakých podmínek. Záleží proto na úvaze zadavatele, jakým způsobem si stanoví rozsah smluvních podmínek. Zadavatel nesmí k vymezení smluvních podmínek přistupovat zcela libovolně, tedy musí při jejich vymezení brát v potaz i základní zásady zadávacího řízení uvedené v ustanovení § 6 zákona, které mají zajistit to, aby smluvní podmínky nebyly zadavatelem formulovány zjevně excesivně.

Rozsudky Nejvyššího správního soudu ze dne 28. 8. 2018, č. j. 9 As 195/2017-47 a ze dne 5. 9. 2018, č. j. 10 As 192/2017-54 se týkají postupu zadavatele při zadávání veřejných zakázek na dodávku laboratorní techniky. Soud v obou případech potvrdil závěr ÚOHS, že zadavatel postupoval v rozporu se zásadou zákazu diskriminace, když v obchodních podmínkách stanovil požadavek na zajištění servisního střediska pro opravy zboží na území ČR, čímž omezil účast v zadávacím řízení dodavatelům, kteří mají sídlo nebo místo podnikání v jiném členském státě Evropské unie či v ostatních státech, které mají s ČR či EU uzavřenu mezinárodní smlouvu zaručující přístup dodavatelům z těchto států k zadávaným částem veřejných zakázek. Tento požadavek dle soudu nebyl racionálně odůvodněn a nebyl nezbytný ani přiměřený ve vztahu k předmětu plnění a sledovanému cíli veřejné zakázky, neboť nebyl nutný k zajištění dostupnosti a kvality servisu, když toho cíle bylo možné dosáhnout méně omezujícími prostředky, aniž by zadavatel vázal geograficky dodavatele pouze na území ČR.

2.9.2 Vztah zadávacích podmínek a smluvního ujednání

V řízeních bez jednacího prvku se typicky uplatní závazný vzor smlouvy, který účastníci zadávacího řízení akceptují bez výhrad; vzor smlouvy bývá doplněn přílohami vymezujícími technické požadavky, režim podpory či rozvoje a související požadavky kybernetické bezpečnosti. Alternativně lze použít i model minimálních standardů obchodních podmínek, které dodavatel závazně promítne do vlastního návrhu smlouvy předkládaného v nabídce. Také v tomto případě však musí být bezpečnostní požadavky zadavatelem formulovány dostatečně určitě a ověřitelně. Vytvoření jasných a vymahatelných smluvních podmínek, včetně reálného harmonogramu a termínu dodání, definovaných metrik výkonnosti (SLA), penalizací za nedodržení závazků a možnosti smluvního exitu (například při fatálním či opakovaném selhání dodavatele) bývají často opatřeními, které by zadavatelé měli precizovat v rámci obchodních podmínek.

Obchodní podmínky musí rovněž transponovat parametry vybraným dodavatelem skutečně nabídnutého plnění, například

- **zařazení členů týmu**, kterým vybraný dodavatel prokazoval technickou kvalifikaci, do seznamu osob, které se budou podílet na realizaci veřejné zakázky na straně dodavatele,
- **identifikace vybraným dodavatelem skutečně nabídnutých** zařízení, programových prostředků, licencí, navržených postupů řešení a dalších podstatných parametrů,
- **provazba mezi identifikovanými členy týmu a nabídnutým plněním** z hlediska odbornosti, odpovědnosti, řízení, schvalování a vlastních pracovních náplní.

Z hlediska kybernetické bezpečnosti proto platí, že bezpečnostní opatření bývají integrální součástí smluvních vztahů. Výslovný pokyn zákonodárce ostatně zní, že poskytovatelé regulované služby (zadavatelé) musí zahrnovat požadavky vyplývající z bezpečnostních opatření do smlouvy uzavírané s dodavatelem (§ 13 odst. 5 ZKB). Zadavatel proto musí zvažovat ve fázi výběru dodavatele, resp. před zahájením zadávacího řízení, jak promítnout obsah požadavků do smluvních podmínek či vzoru smlouvy na plnění veřejné zakázky. Současně platí, že obchodní (smluvní) podmínky není možné uměle oddělit od dalších zadávacích podmínek, jako jsou technické podmínky, o nichž bylo pojednáno shora.

2.9.3 Nastavení smluvních podmínek z hlediska rizik

V případě snahy o řádné nastavení obchodních (smluvních) podmínek bude zpravidla hrát roli hodnocení rizik a volba vhodných opatření (smluvních klauzulí) ke snížení či eliminaci rizika. Základním rizikem (s vysokou závažností) může být nefunkčnost dodávaného plnění při nevhodně smluvně nastaveném procesu implementace poptávaného řešení. V praxi se ukazuje, že v řadě projektů při zavádění či posílení kybernetické bezpečnosti zadavatele je stěžejním opatřením k mitigaci rizika vypracování implementačního projektu (cílového konceptu) v počáteční fázi plnění zakázky. V implementačním projektu (tj. v předimplementační fázi plnění smlouvy) lze rozpracovat a zpřesnit způsob naplnění požadavků na předmět plnění stanovených v zadávacích podmínkách, aniž by docházelo ke změně jejich obsahu. Cílem je vytvořit detailní návrh realizace, který umožní řádné provedení plnění v souladu s nabídkou vybraného dodavatele. Vedle toho by smluvní podmínky implementace ICT řešení měly dbát o zavedení správné akceptační procedury ze strany zadavatele, která by měla zaručit, že plnění bude převzato v souladu s požadavky zadavatele (zadávacími podmínkami i cílovým konceptem).

Právě riziko nedodržení smluvních závazků ze strany vybraného dodavatele bývá často analýzou rizik identifikováno jako hrozba s vysokou úrovní rizikového faktoru. Pokud dodavatel řádně nesplní své závazky, může dojít ke zpoždění nebo přerušení poskytování klíčových služeb, což by mohlo ovlivnit provoz a bezpečnost zadavatele. Opatření pro tuto hrozbu opět spočívají především ve správném nastavení smluvních podmínek a stanovení vhodně zvolených sankcí za jejich nesplnění (např. při odmítnutí součinnosti při incidentu, zásadním porušení pravidel přístupu či poddodavatelského řetězce, opakovaném nedodržení SLA, zmaření auditu), včetně možnosti odstoupení či výpovědi smlouvy. Na místě je vhodné stanovení vysoké úrovně dostupnosti služeb, včetně reakčních dob, režimu poskytování služby a incident managementu (evidence incidentů a pravidelný reporting vůči zadavateli). Lze doporučit, aby SLA (dohoda o úrovni služby) obsahovala

nejen dostupnost, ale i RTO (Recovery Time Objective – maximálně přípustná doba výpadku služby) a RPO (Recovery Point Objective – maximálně přípustná ztráta dat v čase) ve vazbě na kritičnost služby.

2.9.4 Vazba smluvních ujednání na ZKB

Z hlediska ZKB a jeho prováděcích předpisů je pro smluvní oblast zásadní zejména režim poskytování regulované služby (nižší vs. vyšší povinnosti) a dále otázka, zda se na konkrétního dodavatele vztahuje **status tzv. významného dodavatele** (§ 2 písm. h) vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností). U povinných osob v režimu vyšších povinností se očekává aktivní řízení dodavatelů: zadavatel má stanovit bezpečnostní pravidla pro dodavatele, vyžadovat jejich plnění, řídit související rizika a identifikovat a evidovat významné dodavatele; významné dodavatele je třeba prokazatelně informovat o tomto statusu a smlouvy s nimi musí obsahovat relevantní ustanovení podle přílohy č. 5 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Zde platí princip, že zadavatel z katalogu smluvních náležitostí definovaných přílohou č. 5 vybírá jen ty části, které jsou relevantní pro připravovaný smluvní vztah, resp. příslušná smluvní ustanovení blíže konkretizuje dle ad hoc situace (jedná se o typická performativní pravidla, kdy konkrétní opatření si volí zadavatel, který může v odůvodněných případech seznat, že některá oblast není relevantní, a proto všechny vyhláškou definované možnosti nevyužije).

Zároveň platí, že i mimo kategorii významných dodavatelů se zadavateli typicky vyplatí **sjednat základní bezpečnostní klauzule** (auditovatelnost, incident management, poddodávky, vzdálené přístupy, SLA apod.), protože právě smluvní nastavení je „převodníkem“ mezi bezpečnostními požadavky a reálným plněním. U poskytovatelů v režimu nižších povinností se rovněž očekává, že zadavatel do smlouvy s dodavatelem promítne určité požadavky na smluvní ujednání dle přílohy č. 2 k vyhlášce č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Opět i v tomto případě platí, že zadavatel z obsahových náležitostí dané přílohy volí jen ty, které jsou využitelné pro adekvátní nastavení smluvního vztahu s dodavatelem.

2.9.5 Data, licence a poddodavatelé

V rovině bezpečnosti informací by smluvní podmínky měly vymezit, jaká aktiva jsou plněním dotčena a jaké minimální požadavky se na dodavatele kladou (zejména z hlediska důvěrnosti, integrity a dostupnosti informací/dat), včetně pravidel pro řízení přístupů, logování, patch management a práci se zranitelnostmi. Důležitá je i smluvní úprava vzdálené správy a privilegovaných přístupů (např. VPN, administrátorské účty) a závazek dodavatele podřídit se bezpečnostním pravidlům zadavatele nebo předem schváleným politikám.

V oblasti dat je vhodné výslovně vymezit oprávnění k užívání dat, zákazy sekundárního využití, požadavky na lokalitu zpracování/uložení (zejména u cloudu/outsourcingu) a podmínky, za nichž mohou být data předávána třetím osobám či poddodavatelům.

Autorská a licenční ujednání jsou z pohledu kybernetické bezpečnosti důležitá nejen kvůli právu užití, ale i kvůli schopnosti dlouhodobě zajistit údržbu, bezpečnostní aktualizace a případnou změnu

dodavatele bez nepřiměřeného vendor lock-in. Tomu odpovídá také smluvní úprava exitu strategie, když by smlouva měla obsahovat realistický exit plán, pravidla migrace a součinnosti dodavatele při přechodu, požadavky na formáty předání dat a provozních informací a také bezpečné smazání a likvidaci dat po skončení smlouvy.

Pro zajištění vymahatelnosti závazků dodavatele je nezbytné smluvně sjednat právo zadavatele ověřovat plnění bezpečnostních závazků; typicky formou kontroly, zákaznického auditu a testování (v přiměřeném rozsahu podle povahy služby a rizik).

2.10 Zohlednění bezpečnostních požadavků v průběhu plnění smlouvy a změny závazku

2.10.1 Obecný rámec změn smluvního závazku

Předmět veřejné zakázky v oblasti ICT a kybernetické bezpečnosti je často složitým konglomerátem, který se v realizační i provozní fázi dynamicky mění ve vazbě na změny lokálního i světového trhu, bezpečnostní situace, nově identifikované hrozby atd. Řešení problému formou využití stávajících smluv se tedy zpravidla nabízí na prvním místě. V zájmu maximalizace možností pro řešení v oblasti ICT a kybernetické bezpečnosti lze doporučit, aby zadavatel takové možnosti využíval. Z hlediska podrobné klasifikace takových nástrojů lze možnosti zadavatele rozdělit na následující postupy.

2.10.2 Čerpání služeb ze stávající smlouvy

Čerpání služeb ze stávající smlouvy – stávající smlouva, ať již smlouva, na základě které bylo pořízeno původní řešení (smlouva o dílo, smlouva o dodávce ICT systému apod.), případně jiná smlouva, která byla v souvislosti jeho pořízením uzavřena (servisní, rozvojová, provozní apod,), může (resp. v ideálním případě by měla) obsahovat sjednaný určitý počet hodin či člověkodní pro potřebu čerpání služeb implementačních, programátorských, poradenských či obdobných. Jedná se nejčastěji o tzv. měřený kontrakt se sjednaným měsíčním či ročním limitem. Zadavatel má na základě takové smlouvy možnost čerpat řadu důležitých služeb, které mu např. mohou pomoci odpoutat se od určité, nově rizikové technologie, doplnit bezpečnostní řešení systému apod.

2.10.3 Vyhrazené změny závazku

Vyhrazená změna závazku (§ 100 odst. 1 ZZVZ) – obdobně jako smlouvou předvídané mechanismy plnění lze využít tento nástroj ZZVZ k zajištění rozvojových potřeb či změnových požadavků, pokud je zadavatel schopen je předvídat a předem dobře definovat. Na rozdíl od služeb čerpaných dle stávající smlouvy se v případě vyhrazené změny závazku bude jednat o věcně a technicky exaktněji definovaný celek, což vyplývá z požadavků tohoto zákonného ustanovení. Jako vyhrazenou změnu závazku lze ve smlouvě sjednat např. dodatečné pořízení bezpečnostního opatření, výměnu určité rizikové komponenty, dodání paralelního řešení apod. Podstatné v těchto případech je, aby podmínky pro tuto změnu a její obsah byly ve smlouvě jednoznačně vymezeny a změna neměnila celkovou povahu veřejné zakázky.

> *Je třeba akcentovat, že změnový mechanismus v případě vyhrazených změn závazku musí být skutečně určen **dostatečně jasně a srozumitelně**, aby z něj bylo patrno, čeho se má změna týkat a v důsledku čeho k ní má dojít. Tomuto tématu se věnuje např. rozhodnutí ÚOHS uvedené ve věci sp. zn. S0520/2022/VZ, č. j. 40587/2022/500 ze dne 15. 11. 2022. V citovaném rozhodnutí je nad rámec již uvedeného dále dovozeno, že pokud má být přijetí vyhrazené změny podmíněno pouze rozhodnutím zadavatele, musí být navíc jednoznačně stanoveno, za jakých konkrétních okolností, které v průběhu realizace veřejné zakázky nastanou, bude změnové ujednání aktivováno. Je tomu tak proto, aby podobu možných změn ve smlouvě znali dodavatelé již od počátku zadávacího řízení a mohli tomu přizpůsobit svoji nabídku.*

Změnu je rovněž možné vyhradit dle § 100 odst. 2 ZZVZ jako vyhrazenou změnu dodavatele. V oblasti ICT a kybernetické bezpečnosti se nabízí takovou možnost vyhradit, pokud by vybraný dodavatel v průběhu plnění smlouvy přestal splňovat bezpečnostní podmínky, a zadavatel by byl nucen přistoupit k odstoupení od uzavřené smlouvy. Uzavření smlouvy s dalším dodavatelem v pořadí, který bezpečnostní podmínky nadále splňuje by mohlo efektivně vyřešit vzniklý deficit v poskytování regulovaných služeb, který by jinak byl zadavatel nucen asanovat novým zadávacím řízením.

Změnu je rovněž možné vyhradit dle § 100 odst. 3 ZZVZ jako poskytnutí nových služeb nebo nových stavebních prací vybraným dodavatelem za předpokladu, že jsou naplněny podmínky pro použití JŘBU dle § 66 ZZVZ, předpokládaná hodnota nových služeb nebo nových stavebních prací nepřevyšuje 30% předpokládané hodnoty veřejné zakázky a zadavatel v zadávací dokumentaci uvedl dobu a rozsah poskytnutí nových služeb nebo nových stavebních prací. Jedná se tedy ustanovení obdobné ustanovení § 100 odst. 1 ZZVZ, které však v tomto případě lze použít pouze na služby a stavební práce, nikoli na dodávky. Současně platí, že na rozdíl od ustanovení § 100 odst. 1 ZZVZ je předpokladem poskytnutí nového plnění úspěšná realizace JŘBU dle § 66 ZZVZ se stávajícím dodavatelem.

2.10.4 Nepodstatné změny závazku

Pokud smluvně předvídané mechanismy nestačí k řádné správě řešení implementovaného k podpoře kybernetické bezpečnosti a provedení dalších potřebných opatření, jejichž potřebu zadavatele odhalí dodatečně, lze v dalším rozsahu využít změnové mechanismy dle § 222 odst. 4, 5 a 6 ZZVZ (resp. a contrario § 222 odst. 3 ZZVZ).

Změna de minimis (§ 222 odst. 4 ZZVZ) – v případě dodávek a služeb limitovaná 10 % v absolutní hodnotě změny a současně finančním limitem pro nadlimitní veřejnou zakázku. Pokud bude provedeno více změn, je rozhodný součet hodnot všech těchto změn. Může se jednat v podstatě o jakoukoli změnu z vlastního rozhodnutí zadavatele, pokud nemění povahu původní veřejné zakázky a zadavatel její provedení považuje za vhodné. Prakticky je doporučeno tento institut aktivovat ve chvíli, kdy nelze využít smluvní instituty ve stávající smlouvě či vyhrazenou změnu závazku, ať již z toho důvodu, že nebyly vůbec sjednány, případně proto, že tyto instituty již byly kapacitně vyčerpány.

Další nepodstatné změny dle § 222 odst. 5 a 6 ZZVZ – jedná se o tzv. nezbytné dodatečné dodávky a služby, při nemožnosti nebo značné obtížnosti a nákladnosti změny osoby dodavatele (§ 222 odst. 5 ZZVZ), resp. změnu, jejíž potřeba vznikla v důsledku okolností, které zadavatel jednající s náležitou péčí nemohl předvídat, a která nemění celkovou povahu veřejné zakázky (§ 222 odst. 6 ZZVZ). Cenový nárůst související se změnami podle odstavců 5 nebo 6 při odečtení služeb nebo dodávek, které nebyly s ohledem na tyto změny realizovány, nesmí přesáhnout 30 % původní hodnoty závazku; pokud bude provedeno více změn, je rozhodný součet cenových nárůstů všech změn podle odstavců 5 a 6. Otázku, zda je použití příslušného institutu v případě plnění v oblasti ICT a kybernetické bezpečnosti legální, nelze žádným způsobem zobecnit, záležitost je nutné posuzovat v každém případě zvlášť. Obecně lze konstatovat, že použití § 222 odst. 5 ZZVZ je možné například u dodatečných dodávek dalších přístupových licencí informačního systému.

Za změnu okolností, které zadavatelé (ani při vynaložení náležité péče) nemohli předvídat ve smyslu § 222 odst. 6 ZZVZ, bude možné standardně považovat typicky nepředvídané legislativní změny, které zadavatel v rámci provozovaných systémů musí zohlednit, anebo další informace získané z vnějšího prostředí, například ve formě varování NÚKIB, pokud musí být zohledněna dodatečně i v existujících smluvních vztazích. Pokud regulovaná osoba (zadavatel) pravidelně provádí hodnocení rizik i v průběhu plnění, tj. během trvání smluvního vztahu, může totiž dojít ke zjištěním vyvolávajícím nezbytnost zasáhnout do uzavřeného smluvního vztahu a provést změny smlouvy dle uvedeného ustanovení.

2.10.5 Změna plnění a technologická substituce

Změna dle § 222 odst. 7 ZZVZ – záměna jedné nebo více položek plnění je sice připuštěna jen v případě soupisu stavebních prací za splnění určitých předpokladů, avšak optikou § 222 odst. 3 ZZVZ je tato záměna aplikovatelná i na dodávky a služby, tedy i v oblasti ICT a kybernetické bezpečnosti (např. v případě nedostupnosti IT produktu dle nabídky dodavatele a jeho nahrazení nástupnickou řadou stejné či lepší kvality za stejnou či nižší cenu).

3 Omezení účasti dodavatelů ze třetích zemí

3.1 Právní regulace

Zadávací směrnice Evropské unie, návazně ZZVZ, jsou založeny na zásadě rovného zacházení a zásadě zákazu diskriminace, jež se uplatní i ve vztahu ke státní příslušnosti dodavatelů a původu zboží. Dle § 6 odst. 3 ZZVZ zadavatel nesmí omezovat účast v zadávacím řízení těm dodavatelům, kteří mají sídlo v

a) členském státě Evropské unie (EU), Evropského hospodářského prostoru (EHP) nebo Švýcarské konfederaci, nebo
b) v jiném státě, který má s Českou republikou nebo s Evropskou unií uzavřenu mezinárodní smlouvu zaručující přístup dodavatelům z těchto států k zadávané veřejné zakázce. Mezi tyto dohody patří primárně tzv. The Agreement on Government Procurement (GPA) dohoda, jejímiž signatáři je řada zemí mimo EU, EHP a Švýcarskou konfederaci. Rovný přístup může být dále zaručen kandidátským státům Evropské unie, případně jiným státům na základě dalších dohod.

Á contrario má tedy zadavatel právo vyloučit účastníka se sídlem mimo teritoria definovaná výše uvedenými písmeny a) a b) z účasti v zadávacím řízení, a to i v případě, že pro takové vyloučení nemá věcný důvod například vyplývající z analýzy rizik. Rozhodnutí je omezeno výhradně na autonomii vůle zadavatele.

V případě sektorových veřejných zakázek obsahuje § 168 ZZVZ pravidla vyloučení účastníků zadávacího řízení veřejné zakázky na dodávky, jejichž nabídka obsahuje dodávky původem ze třetích zemí, a znevýhodnění takových účastníků zadávacího řízení při hodnocení nabídkové ceny.

Významné upřesnění pak do celé problematiky vnesl rozsudek Soudního dvora Evropské unie ze dne 22. 10. 2024 ve věci C-652/22 Kolin Inşaat Turizm Sanayi ve Ticaret. Na základě tohoto soudního rozhodnutí vydal ÚOHS metodiku „Možnost zadavatele definovat účast dodavatele ze třetí země v zadávacím řízení, závěry vyplývající z rozsudku SDEU C-652/22 Kolin“. Tato metodika nabízí řadu možných individuálních omezujících opatření globálního i partikulárního charakteru, které je možné vůči dodavatelům ze třetích zemí uplatnit.

Obecně je možné doporučení shrnout tak, že

- zadavatel může stanovit v zadávacích podmínkách zákaz účasti dodavatelů ze třetích zemí, a to dodavatelům ze všech těchto zemí, nebo jen z některých z nich,
- pokud zadavatel v zadávacích podmínkách omezující podmínku nestanoví, je účast dodavatelů ze třetích zemí připuštěna,
- pokud zadavatel účast dodavatelů ze třetích zemí připustí (tj. nestanoví podmínku účasti, která jejich účast v zadávacím řízení vylučuje), může se rozhodnout, zda k nim bude v zadávacím řízení přistupovat rovným způsobem, jako k dodavatelům z členských států EU, či zda vůči nim přijme znevýhodňující opatření, a to k dodavatelům ze všech těchto zemí,

nebo jen z některých z nich; případná znevýhodňující opatření musí být v souladu se zásadou transparentnosti vymezena v zadávacích podmínkách,

- znevýhodňujícími opatřeními vůči dodavatelům ze třetích zemí mohou být například
  - úprava bodového hodnocení v neprospěch dodavatelů ze třetích zemí,
  - přísnější požadavky na prokázání kvalifikace,
  - přísnější požadavky na obsah nebo formu předkládaných dokladů,
  - přísnější obchodní nebo smluvní podmínky (například záruky, smluvní pokuty, pojištění).

Pravidla pro vyloučení některých dodavatelů nebo omezující opatření mohou být založena na původu dodavatele (fyzické nebo právnické osoby), nebo na původu dodávaného zboží, přičemž

- při formulaci vymezení okruhu vyloučených dodavatelů, nebo dodavatelů, vůči nimž směřují omezující opatření, lze vycházet například z čl. 3 odst. 1 Nařízení (EU) 2022/1031 (viz kapitola 3.2),
- při formulaci omezení vztahujícího se k původu zboží lze vycházet například z § 168 odst. 1 ZZVZ,
- omezující opatření se mohou vztahovat i na poddodavatele účastníka zadávacího řízení, přičemž lze při jeho formulaci vycházet například z čl. 8 odst. 1 Nařízení (EU) 2022/1031 (viz kapitola 3.2). V případě opatření proti poddodavatelům by měla být připuštěna výměna poddodavatele, na základě pravidel, které je možné stanovit obdobně jako v § 85 odst. 2 ZZVZ.

Obecně je ve vztahu k této problematice nutné upozornit na úskalí toho, jakým způsobem zadavatel skutečně definuje omezující opatření, založené na původu dodávaného zboží a jak formulovat okruh vyloučených (znevýhodněných) dodavatelů. Předpisy dávají v této věci poměrně velkou autonomii, kdy exkluze nebo znevýhodnění mohou být založeny na územně-geopolitické dimenzi (např. místo výroby) nebo ekonomicko-institucionální dimenzi (např. vlastnická struktura výrobního podniku), nicméně je nutné upozornit na potenciální následné problémy se skutečným ověřováním naplnění stanovených pravidel v průběhu zadávacího řízení. Interpretační nejistota může vyplývat z řady důvodů (např. nedostatečná trackovatelnost výroby v třetí zemi, nedohledatelnost vlastnické struktury podniku) a následně je pak možné předpokládat (bez ohledu na oprávněnost zadavatelem nastavené exkluze či znevýhodnění) i obranu relevantních dodavatelů, s potenciálním správním a soudním přezkumem.

Výše zmíněná autonomie vůle zadavatele při řízené diskriminaci dodavatelů ze třetích zemí je však dále v některých taxativních případech dokonce usměrněna na povinnost takového účastníka vyloučit, a to v případech, uvedených v následující kapitole.

3.2 Mezinárodní sankce

Vedle vlastního zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti a aplikace požadavků, protiopatření a bezpečnostních opatření plynoucích ze ZKB vstupuje do celé problematiky skupina legislativních opatření, vydaná v rámci zajišťování provádění mezinárodních sankcí za účelem udržování mezinárodního míru a bezpečnosti, ochrany základních lidských práv a boje proti terorismu, která je v právním řádu ČR uvozována zákonem č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů. Do ZZVZ je problematika mezinárodních sankcí promítnuta prostřednictvím § 48a ZZVZ, který upravuje nezadání veřejné zakázky účastníku zadávacího řízení, pokud je to v rozporu s mezinárodními sankcemi.

Oblast mezinárodních sankcí zahrnuje v dlouhodobém horizontu velké množství sankčních mechanismů, jako jsou opatření ve vztahu k afghánskému hnutí Talibán, k Irácké republice, mezinárodní sankce vůči Rusku a Bělorusku a řada dalších mezinárodních sankcí, které lze v celosvětovém měřítku se všemi relevantními souvislostmi rovněž nalézt na webu https://www.sanctionsmap.eu/#/main. Některé mezinárodní sankce lze z aktuálního pohledu již považovat za relativně „vyhaslé“, jiné naopak za velice aktuální.

Z hlediska § 48a ZZVZ zadavatel nezadá veřejnou zakázku účastníku zadávacího řízení, pokud je to v rozporu s mezinárodními sankcemi. Pokud se tedy mezinárodní sankce vztahuje na účastníka zadávacího řízení, může ho zadavatel vyloučit z účasti v zadávacím řízení, resp. pokud se vztahuje na vybraného dodavatele, vyloučí ho zadavatel z účasti v zadávacím řízení. Pokud se mezinárodní sankce vztahuje na poddodavatele účastníka zadávacího řízení, může zadavatel požadovat nahrazení poddodavatele, pokud se vztahuje na poddodavatele vybraného dodavatele, musí zadavatel požadovat nahrazení poddodavatele. Tyto sankce je třeba posuzovat jak ve vztahu k poddodavatelům, kterými je prokazována kvalifikace, tak i ve vztahu k běžným poddodavatelům, podílejícím se na plnění veřejné zakázky, a to kdekoliv v poddodavatelském řetězci (za předpokladu, že jsou zadavateli známi).

Dle § 130 ZZVZ se zákaz zadat zakázku subjektu, na který se aplikují mezinárodní sankce, v rozsahu § 48a odst. 1 uplatní i v rámci zvláštních postupů, a to v tzv. minitendrech na základě rámcových dohod a v dynamickém nákupním systému. V případě soutěže o návrh je stanoveno samostatné pravidlo postupu v případě uplatnění mezinárodních sankcí v § 148 odst. 8 ZZVZ.

Vlastní ověření, zda se na účastníka zadávacího řízení, vybraného dodavatele či všechny relevantní poddodavatele mezinárodní sankce skutečně vztahují, mohou zadavatelé v zadávacím řízení řešit různými způsoby, např.

- ověřením účastníka v evidenci skutečných majitelů,
- ověřením účastníka v sankčních rejstřících (např. Datlab),
- smluvním zavázáním dodavatele k prověřování jeho poddodavatelů a k nezpřístupnění finančních prostředků, obdržených za plnění veřejné zakázky, přímo ani nepřímo osobám, subjektům či orgánům uvedeným v sankčních seznamech, a to v rozsahu relevantních sankčních nařízení,

- vyžádáním čestného prohlášení účastníka o nepřítomnosti na sankčních seznamech, prověřování poddodavatelů a nezpřístupnění finančních prostředků, obdržených za plnění veřejné zakázky, přímo ani nepřímo osobám, subjektům či orgánům uvedeným v sankčních seznamech, a to v rozsahu relevantních sankčních nařízení, anebo
- dalšími možnými způsoby dle konkrétní situace a při zachování základních zásad zadávání veřejných zakázek.

Aktuálně do oblasti veřejných zakázek nejvíce dopadají mezinárodní sankce vůči Rusku a Bělorusku, a to v souvislosti s válkou na Ukrajině. Tyto sankce lze rozdělit do dvou skupin:

1) **Individuální finanční sankce** – zaměřeny vůči konkrétním subjektům z Ruska a Běloruska a subjektům s nimi spojeným, uvedeným na sankčních seznamech, přičemž spočívají v zmrazení a zákazu zpřístupnění finančních prostředků a hospodářských zdrojů sankcionovaných osob. Individuální finanční sankce dopadají na všechny veřejné zakázky bez ohledu na jejich předpokládanou hodnotu. Uplatní se tedy i na veřejné zakázky malého rozsahu. Individuální finanční sankce jsou upraveny v nařízení Rady (EU) č. 269/2014 a nařízení Rady (EU) č. 208/2014. Jmenný seznam s odůvodněním a datem zařazení je obsažen vždy v přílohách příslušného nařízení. Individuální finanční sankce v případě Běloruska jsou obsaženy v nařízení Rady (ES) č. 765/2006.
2) **Ekonomické sankce** – ekonomické sankce nemají vazbu na sankční seznamy osob, uplatní se tedy za daných podmínek obecně, přičemž v oblasti zadávání veřejných zakázek spočívají v sankcích přímo zaměřených na oblast zadávání a plnění veřejných zakázek spočívajících v zákazu zadat a plnit veřejné zakázky subjekty uvedenými v čl. 5k nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým došlo ke změně „základního“ nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, včetně poddodavatelů v celém poddodavatelském řetězci, v případě poddodavatelů v rozsahu převyšujícím 10 % hodnoty zakázky.

Vedle sankcí zaměřených vůči Rusku a Bělorusku platí Nařízení Evropského parlamentu a Rady (EU) 2022/1031 ze dne 23. června 2022 o přístupu hospodářských subjektů, zboží a služeb třetích zemí na trhy Unie s veřejnými zakázkami a koncesemi a o postupech na podporu jednání o přístupu hospodářských subjektů, zboží a služeb Unie na trhy třetích zemí s veřejnými zakázkami a koncesemi (tzv. IPI – International Procurement Instrument, nástroj pro mezinárodní zadávání veřejných zakázek), které omezuje přístup na trh EU pro dodavatele z třetích zemí.

Na toto Nařízení navazuje první praktické využití tohoto nástroje, kterým je Prováděcí nařízení Komise (EU) 2025/1197 ze dne 19. června 2025, kterým se ukládá opatření v rámci nástroje pro mezinárodní zadávání veřejných zakázek omezující přístup hospodářských subjektů a zdravotnických prostředků pocházejících z Čínské lidové republiky na trh Evropské unie s veřejnými zakázkami na zdravotnické prostředky podle nařízení Evropského parlamentu a Rady (EU) 2022/1031. Toto nařízení zavádí od 30. 6. 2025 omezení účasti dodavatelů a zdravotnických prostředků Čínské lidové republiky v zadávacích řízeních na veřejné zakázky v EU, jejichž hodnota překračuje 5 milionů eur, což má zajistit férovější podmínky pro evropské dodavatele a zajistit reciproční přístup na relevantní trhy.

4 Obecná doporučení

Plně využívejte možnosti, které Vám ZZVZ dává

ZZVZ nabízí zadavatelům různé možnosti, jak chránit své zájmy. Tyto jsou však často zadavateli nevyužity. Jedná se například o možnost ochrany citlivých informací, které jsou součástí zadávací dokumentace nebo možnost postupného zužování okruhu dodavatelů vylučováním těch méně vhodných v rámci vícefázových řízení s jednacím prvkem (zejména soutěžního dialogu nebo jednacího řízení s uveřejněním). Je třeba apelovat na zadavatele, aby byli plně seznámeni se všemi možnostmi, které jim ZZVZ při zadávání veřejných zakázek nabízí, resp. zákonné instrumenty v potřebném rozsahu efektivně využívali.

Odůvodněte si každý krok zadávacího řízení

Zadávací řízení je velmi formální proces, který klade značné nároky na zadavatele co do naplnění zákonných požadavků. Obecně však platí, že cílem ZZVZ není zadavatele pouze svazovat pravidly ve prospěch široké hospodářské soutěže, nýbrž ZZVZ zadavatelům dává i možnosti, jak chránit své legitimní zájmy. Tyto však musí být podloženy logickými a pevnými argumenty. Proto je nutné apelovat na to, aby byl každý krok zadavatele odůvodněný racionálními důvody a tyto důvody byly (s ohledem na zásadu transparentnosti a možnost pozdějšího přezkumu) řádně zdokumentovány. Pokud zadavatel bude schopen rozumně a věcně zdůvodnit každý svůj krok v rámci zadávacího řízení, přináší mu to značnou výhodu při případném přezkumu a dokáže urychlit celý přezkumný proces.

Veškeré podmínky plnění a požadavky zadavatele se musí promítat do obchodních podmínek a být řádně zajištěny

Z hlediska jednotlivých částí zadávací dokumentace jsou pro vymezení jasných obchodních podmínek klíčové zejména následující oblasti

- provázání zadávacích podmínek se smlouvou
    - provázání podmínek kvalifikace na obchodní podmínky (zanesení jednotlivých členů realizačního týmu z nabídky vybraného dodavatele do smlouvy apod.),
    - provázání technických podmínek předmětu veřejné zakázky na obchodní podmínky (vlastní technická specifikace jako příloha smlouvy),
    - provázání nabídnutých parametrů, který byly hodnoceny, na obchodní podmínky,
    - provázání vybraným dodavatelem skutečně nabídnutého plnění do původní technické specifikace předmětu veřejné zakázky a následný propis do obchodních podmínek (výčet skutečně nabídnutých výrobků, licencí a postupů apod.),
    - jasné definovaní rolí, odpovědností a pravomocí členů realizačního týmu s bezprostřední vazbou na technickou specifikaci (který člen realizačního týmu zodpovídá za jakou část implementace, na realizaci jakých zařízení a programových prostředků se bezprostředně podílí, odpovědnost za akceptaci konkrétní části plnění apod.)

- jednoznačně, nediskriminačně a reálně nastavený harmonogram s jasně definovanými milníky, které vymezují klíčové fáze realizace předmětu plnění a logicky jej člení do jednotlivých etap, přičemž celý harmonogram je integrální součástí smlouvy,
- jednoznačně, nediskriminačně a reálně nastavené podmínky SLA, dostupnosti, záruky, servisu, maintenance a technické podpory, které jsou integrální součástí smlouvy, popř. součástí samostatné smlouvy,
- ustanovení vhodných zajišťovacích a sankčních mechanismů pro efektivní naplnění všech výše uvedených bodů.

Plňte řádně povinnosti vyplývající ze zákona o kybernetické bezpečnosti

ZZVZ říká „jak" mají zadavatelé své nákupy provést, nikoli „co" mají zadavatelé poptávat. Naopak ZKB a jeho prováděcí předpisy regulují kvalitativní stránku informačních systémů a zařízení, které zadavatelé používají a poptávají. Požadavky na předmět plnění veřejné zakázky založené na řádném plnění povinností vyplývajících ze ZKB, zejm. na řádně provedeném procesu řízení rizik a výběru bezpečnostních opatření k zajištění požadované úrovně kybernetické bezpečnosti, pak nemohou být z podstaty věci (stejně jako v případě všech dalších požadavků zadavatelů založených na plnění jejich zákonných povinností) považovány za neodůvodněné.

Dobrovolné zohlednění požadavků zákona o kybernetické bezpečnosti

Zadavatelé, na něž se osobní působnost ZKB formálně nevztahuje, mohou bezpečnostní rámec tohoto zákona a jeho prováděcích právních předpisů využít jako osvědčenou dobrou praxi pro přiměřené nastavení zadávacích podmínek, zejména v oblasti řízení rizik, ochrany informací a řízení dodavatelů. Takový postup sám o sobě nepředstavuje porušení zásad zadávání veřejných zakázek ani neodůvodněnou diskriminaci dodavatelů, pokud je založen na objektivních potřebách zadavatele a na konkrétních okolnostech dané veřejné zakázky.

Rozhodovací praxe ÚOHS přitom potvrzuje, že při posuzování zákonnosti bezpečnostních požadavků není rozhodující, zda je zadavatel povinnou osobou podle zákona o kybernetické bezpečnosti, ale zda omezení hospodářské soutěže sleduje legitimní cíl, je přiměřené a je založeno na racionálně zdůvodněných a přezkoumatelných úvahách zadavatele. Zadavatel by proto měl být schopen doložit, z jakých rizik vycházel a proč zvolil konkrétní bezpečnostní požadavky, a to i v případě jejich dobrovolného převzetí z rámce zákona o kybernetické bezpečnosti.

5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
9. června 2026	1.0	OREG, ÚOHS, ApVZ	Vytvoření dokumentu