NÁVRH MECHANISMU POSUZOVÁNÍ A OMEZOVÁNÍ RIZIK SPOJENÝCH S DODAVATELI DO INFRASTRUKTURY ELEKTRONICKÝCH KOMUNIKACÍ

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

17. BŘEZNA 2022

VERZE DOKUMENTU: 1.0

NÁVRH MECHANISMU POSUZOVÁNÍ A OMEZOVÁNÍ RIZIK SPOJENÝCH S DODAVATELI DO INFRASTRUKTURY ELEKTRONICKÝCH KOMUNIKACÍ

Rozpracování „Prověřování bezpečnostní spolehlivosti dodavatelů“ za účelem přípravy věcného záměru zákona na základě usnesení Bezpečnostní rady státu č. 33 ze dne 19. října 2021

UPOZORNĚNÍ:

Tento dokument je pracovní verzí návrhu, vycházejícího z materiálu projednaného Bezpečnostní radou státu. Do tohoto dokumentu jsou průběžně zapracovávány úpravy vycházející z diskusí a konzultací se zástupci soukromého sektoru v oblasti elektronických komunikací a organizačních složek státu, **dokument nepředstavuje finální či závazné znění návrhu a nelze z něj vyvozovat závěry o budoucí podobě právních předpisů** či současném nebo budoucím postupu státu.

Obsah

1 Úvod

Bezpečnostní rada státu (dále jen „**BRS**“) projednala dne 19. října 2021 varianty postupu naplnění opatření SM03 Souboru opatření EU pro kybernetickou bezpečnost sítí 5G (tzv. EU 5G Toolbox), obsažené v materiálu „Posuzování a omezování rizik spojených s dodavateli 5G sítí: Varianta 2 a 3“, č. j.: 34158/2021-UVCR (dále jen „**Koncepce**“), a svým usnesením č. 33 ze dne 19. října 2021 vybrala variantu 2 – „Prověřování bezpečnostní spolehlivosti dodavatelů“ k dalšímu rozpracování do podoby věcného záměru zákona.

Tento dokument představuje pracovní návrh rozpracování výše uvedené varianty Koncepce (dále jen „**Návrh**“) **zpracovaný pro účely konzultace a diskuse o návrhu se zástupci soukromého sektoru v oblasti elektronických komunikací a organizačních složek státu** a jeho pozdějšího zpracování do podoby věcného záměru zákona Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) jako předkladatelem a Ministerstvem vnitra, Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí, Českým telekomunikačním úřadem, Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím jako spolupředkladateli.

Návrh se zaměřuje na představení samotného navrhovaného mechanismu posuzování a omezování rizik spojených s dodavateli 5G sítí (dále jen „**Mechanismus**“) bez uvedení plného kontextu dění na mezinárodní a národní úrovni, jež návrhu přecházelo a přispělo k potřebě jeho vzniku. Odůvodnění potřebnosti vzniku Mechanismu bude nicméně rozvedeno v příslušných fázích legislativního procesu.

2 Manažerské shrnutí

- Návrh představuje Mechanismus coby **možnou podobu vnitrostátního přístupu k prověřování dodavatelů** do infrastruktury elektronických komunikací.
- Mechanismus vychází z vnitrostátní i mezinárodní potřeby a obsahuje jak nové instituty a procesy, tak prvky **stávajících vnitrostátních regulací** v oblasti bezpečnosti a **zahraničních příkladů dobré praxe**.
- Mechanismus je navržen jako součást stávajícího systému zajišťování kybernetické bezpečnosti v České republice, právně upraveného zejména **zákonem o kybernetické bezpečnosti** a prováděcí **vyhláškou o kybernetické bezpečnosti**.
- S pomocí stávajících právních definic vymezuje Návrh subjekty, které budou Mechanismem prověřovány (Přímí dodavatelé a Poddodavatelé), plnění, pro která bude nezbytné využít pouze prověřené subjekty (Bezpečnostně relevantní dodávky), subjekty, jež budou povinny prověřené subjekty využívat (Odběratelé) a části systémů těchto subjektů, ve vztahu, k nimž bude tato povinnost existovat (Kritická součást systému).
- Proces prověření Mechanismem (řízení o prověření) **vychází z obecné úpravy správního řízení** se speciální úpravou v některých oblastech. Řízení o prověření **zahajuje primárně žadatel** (Přímý dodavatel) po prokázání potenciálu dodání Bezpečnostně relevantní

dodávky a po předložení povinného rozsahu informací; **alternativně je řízení o prověření zahájeno z moci úřední** při změně okolností předchozího prověření nebo v důsledku kontrolního zjištění.

- V rámci prověření vyhodnocují zapojené orgány státní správy **naplnění definovaných kritérií** ve vztahu k Přímému dodavateli a jeho dodavatelskému řetězci (Poddodavatelé). Výsledné rozhodnutí o prověření stanoví **kategorii identifikované bezpečnostní rizikovosti** Přímého dodavatele a jeho Poddodavatelů a případně ukládá **povinná opatření** při využití daných dodavatelů Odběratelem; alternativně zakazuje využití rizikových dodavatelů. Proti rozhodnutí o prověření je možné se bránit prostřednictvím mimořádných opravných prostředků či ve správním soudnictví.
- Pro přiměřené vyvážení urgence zajištění bezpečnosti kritické informační infrastruktury a minimalizace dopadu Mechanismu na podnikatelské prostředí obsahuje Návrh **lhůty v řádu roků** pro zohlednění výstupů z prověření Mechanismem v obchodních aktivitách všech příslušných podnikatelů v sektoru elektronických komunikací.

3 Základní rysy Mechanismu

Cílem Mechanismu je účinné **prověřování dodavatelů do strategicky významné komunikační infrastruktury v České republice (dále také „ČR"), vyhodnocení jejich bezpečnostní spolehlivosti a určení opatření ke zmírnění případných identifikovaných rizik**. Mechanismus má také umožnit omezit či vyloučit z dodávek subjekty, které budou vyhodnoceny jako vysoce rizikové, aby byla telekomunikační infrastruktura v ČR, a to zejména 5G sítě, která spadá do regulace zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**"), budována na technologiích důvěryhodných dodavatelů.

Mechanismus je žádoucí a potřebný, jelikož v současné době na národní úrovni neexistuje komplexní mechanismus pro hodnocení rizikového profilu dodavatelů a případné omezení přístupu rizikových subjektů k důležité infrastruktuře státu. Obdobný mechanismus přitom v současnosti není možné připravovat na nadnárodní úrovni, například na úrovni Evropské unie (dále jen „**EU**"), jelikož cílí k zajištění vnitřní bezpečnosti České republiky, která je výlučnou oblastí její odpovědnosti.[1]

Ke stejnému cíli jako Mechanismus zdánlivě směřuje i v současnosti zaváděný evropský systém certifikace kybernetické bezpečnosti[2] a plánované certifikační schéma pro 5G sítě. Na rozdíl od Mechanismu tento systém ale zahrnuje pouze technickou certifikaci produktů, služeb a procesů a neřeší rovinu strategické důvěryhodnosti osoby dodavatele. Evropský systém certifikace

[1] Viz např. čl. 72 Smlouvy o fungování EU.

[2] Tento systém je v zaváděn na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti").

kybernetické bezpečnosti se tedy v současnosti jeví jako vhodný doplněk Mechanismu, avšak nemůže a ani nemá ambice jej nahradit.

Mechanismus prověřování vychází z těchto principů a sleduje tyto cíle:

- **Identifikace a omezení známých případů či existujícího rizika ingerence státních aktérů** do produktů, služeb či procesů prostřednictvím dodavatelů či poddodavatelů, s cílem narušení bezpečnosti (včetně dostupnosti) strategické informační a komunikační infrastruktury státu. Informace o takových případech či rizicích ingerence vychází v mnohých případech z neveřejných zdrojů a vyžadují komplexní technickou a geopolitickou analýzu citlivých informací, kterou je v požadované míře schopen a oprávněn provádět pouze stát, resp. specifické státní instituce.
- **Prověření jako služba státu pro mobilní operátory**. Skutečnost, že Mechanismus prověřuje a identifikuje přítomnost strategického rizika důvěryhodnosti dodavatele, významně omezí riziko narušení důvěrnosti, dostupnosti či integrity informací přenášených systémem, do kterého dodávka směřuje, z neobchodních či netechnických důvodů, jejichž identifikace a posouzení povětšinou není v možnostech a schopnostech mobilního operátora jakožto odběratele.
- **Ponechání problematiky komplexního zajištění bezpečnosti na správci systému či sítě**. V souladu se stávajícím nastavením systému zajišťování kybernetické bezpečnosti v ČR je klíčovým prvkem Mechanismu systém řízení rizik dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**VKB**“). Ačkoliv Mechanismus přichází s novým vstupem státu do tohoto systému, převážnou část identifikace a hodnocení hrozeb a rizik v oblasti kybernetické bezpečnosti ponechává na odpovědnosti operátorů jakožto povinných osob dle ZKB.
- **Minimalizace ekonomických nákladů a princip efektivity**. Mechanismus je vytvářen s cílem minimalizovat ekonomické náklady pro soukromé subjekty i pro stát na úroveň nezbytnou pro zajištění účelu Mechanismu, tedy identifikace a omezení rizik spojených s dodavateli 5G sítí. Mechanismus dále vychází z obecně přijímaného předpokladu, že rizika v oblasti kybernetické bezpečnosti nelze zcela eliminovat, ale pouze omezovat. Mechanismus je tedy navržen tak, aby ve všech částech svého procesu poměřoval náklady a přínosy dané části procesu i Mechanismu jako celku.

4 Vymezení subjektů a předmětu prověřování Mechanismu

Pro vymezení subjektů a předmětu prověřování Mechanismu definuje návrh několik základních pojmů. Tzv. Odběratelé (viz část 4.1 Návrhu) jsou orgány či osoby, které budou mít dle Návrhu povinnost využívat do vymezených částí své infrastruktury (tzv. Kritické součásti systému, viz část 4.2 Návrhu) pouze dodavatele prověřené Mechanismem. Povinnost prověření Mechanismem se

nicméně nebude vztahovat na všechny dodavatele, ale pouze na ty, kteří budou dodávat tzv. Bezpečnostně relevantní dodávky (viz část 4.3.1 Návrhu).

4.1 Odběratel

Odběratelem je orgán či osoba:
která zajišťuje síť elektronických komunikací[3] zajišťující přímé připojení ke kritické informační infrastruktuře.

Rozsah Odběratelů, jejichž dodavatelé budou Mechanismem prověřováni, stanovuje tento Návrh v návaznosti na konzultace s podnikateli, zajišťujícími veřejné komunikační sítě. Rozsah Odběratelů je tímto Návrhem stanoven jak na orgány a osoby, které zajišťují sítě elektronických komunikací a jsou zároveň správci či provozovateli informačního nebo komunikačního systému kritické informační infrastruktury, tak na orgány a osoby, jejichž sítě elektronických komunikací pouze zajišťují správcům a provozovatelům informačních a komunikačních systémů kritické informační infrastruktury konektivitu ke službám elektronických komunikací; obě tyto skupiny subjektů jsou přitom povinnými osobami dle ZKB.[4]

Stanovením užšího rozsahu Odběratelů, jejichž dodavatelé budou prověřováni, například pouze na orgány a osoby, které jsou správci či provozovateli informačního či komunikačního systému kritické infrastruktury a zároveň zajišťují veřejnou komunikační síť, by z prověření Mechanismem vyňalo některé důležité subjekty, zajišťující připojení prvků kritické informační infrastruktury. Stanovení širšího rozsahu Odběratelů, například na všechny subjekty zajišťující síť či službu elektronických komunikací v ČR, se zase v současnosti nejeví jako přiměřené vzhledem k cíli Mechanismu přispívat k zabezpečení strategicky nejvýznamnější infrastruktury, ani vzhledem k sledovanému principu efektivity. Navrhovaný rozsah pojmu Odběratel tak postihuje všechny subjekty, které jsou z hlediska zajištění bezpečnosti strategicky nejvýznamnější telekomunikační infrastruktury České republiky významné, aniž by přitom dopadal na jakékoliv jiné subjekty.

4.2 Rozsah dotčených součástí systému Odběratele

Kritickou součástí systému jsou:
technická aktiva informačního a komunikačního systému[5] Odběratele, **na kterých je,** bez ohledu na zavedení bezpečnostních opatření[6], **závislé připojení kritické informační infrastruktury** do sítě elektronických komunikací (dále jen „**Kritická součást systému**“).

Navrhované vymezení Kritické součásti systému, na jejíž dodávky Mechanismus dopadne, není s ohledem na celkovou provázanost telekomunikační infrastruktury omezeno pouze na prvky mobilních sítí 5. generace, ale na relevantní technická aktiva celé telekomunikační infrastruktury

[3] Ve smyslu § 2 písm. b) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.
[4] § 3 písm. a) až d) ZKB.
[5] Ve smyslu § 2 písm. k) VKB, vyjma objektů, ve kterých jsou systémy umístěny.
[6] Ve smyslu § 4 odst. 1 a násl. ZKB

Odběratele. Těmito relevantními aktivy jsou technické vybavení, komunikační prostředky a programové vybavení, na jejichž správném a spolehlivém fungování je závislé připojení kritické informační infrastruktury k síti elektronických komunikací.

Konkrétní rozsah Kritických součástí systému bude v souladu se stávající systematikou řízení aktiv dle § 4 VKB založen primárně na identifikaci aktiv Odběratelem. Základem Kritické součásti systému sice budou povinná typová aktiva stanovená prováděcím předpisem, konkrétní rozsah aktiv spadajících do Kritické součásti systému však bude vždy individuální a bude vycházet z identifikace aktiv svého informačního a komunikačního systému Odběratelem. Tento přístup ke stanovení rozsahu Kritické součásti systému ponechává identifikaci bezpečnostně relevantních aktiv v maximální možné míře na performativních pravidlech ZKB a VKB a tedy na Odběrateli, vycházeje přitom z předpokladu, že právě Odběratel zná svůj systém nejlépe a je proto nejlépe schopen stanovit postup výběru aktiv zásadních pro bezpečnost jím zajišťované sítě elektronických komunikací.

Zavádění bezpečnostních opatření může mít v některých případech vliv na závislost technického aktiva pro připojení kritické informační infrastruktury. Předmětem prověřování Mechanismem jsou však podle Návrhu všechna technická aktiva, na nichž je připojení závislé z pohledu inherentních rizik. Povinnost zavedení bezpečnostních opatření, jež může hodnotu závislosti technického aktiva pro připojení změnit, je totiž jedním z možných výstupů Mechanismu (viz část 0 Návrhu).

Odběratelům, na které se dosud nevztahovala povinnost zavádění bezpečnostních opatření dle VKB, tedy nově vznikne povinnost identifikace a hodnocení aktiv ve smyslu § 4 VKB. K zavedení nových povinností pro určitý okruh osob či orgánů regulovaných dle ZKB, a to vč. orgánů či osob dle § 3 písm. a) a b) ZKB, kteří spadají do definice Odběratele (viz část 4.1 Návrhu), nicméně dojde s největší pravděpodobností i důsledkem transpozice chystané aktualizace směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „NIS 2“). Jelikož však nejsou rozsah a hloubka nových povinností dle NIS 2 dosud známé, nelze vyloučit, že by mohl těmto subjektům nově uložit povinnost identifikace a hodnocení aktiv dle § 4 VKB namísto NIS 2 již samotný Mechanismus. Mechanismus ovšem v žádném případě nebude rozšiřovat okruh Odběratelů nad rámec osob či orgánů regulovaných dle ZKB podle jeho v současnosti platného právního stavu.

Odběratel – přehled změn ve srovnání s Koncepcí:

- **Zaveden pojem „Odběratel“, jehož význam zůstává shodný jako „povinná osoba mechanismu“ v Koncepci.**
- **Namísto původní kombinace definice operátora dle ZEK a povinných subjektů ze ZKB byla definice Odběratele zjednodušena, užití pojmového aparátu ZEK a ZKB však bylo zachováno. Jedinou definiční podmínkou je nyní poskytování konektivity KII.**
- **Zaveden pojem „Kritická součást systému“, který omezuje dopad Mechanismu pouze na tu část systému Odběratele, která je kritická pro připojení KII k síti elektronických komunikací.**

4.3 Dodavatelský řetězec

Pro vymezení subjektů a předmětu prověřování Mechanismu definuje Návrh také tzv. Bezpečnostně relevantní dodávky a jejich dodavatele, tzv. Přímé dodavatele a jejich tzv. Poddodavatele, na které povinnost prověření Mechanismem dopadne.

4.3.1 Bezpečnostně relevantní dodávka

Bezpečnostně relevantní dodávkou je:

plnění, spočívající ve vývoji, výrobě, sestavení či servisu technického vybavení či komunikačního prostředku s výpočetní kapacitou nebo programového vybavení, **směřující do Kritické součásti systému.**

4.3.2 Prověřovaní dodavatelé

Přímým dodavatelem je:

orgán či osoba, která **na základě smluvního vztahu mezi ní a Odběratelem či osobou propojenou s Odběratelem** prostřednictvím podnikatelského seskupení[7], Odběrateli **poskytuje či umožňuje poskytnutí, anebo má potenciál poskytnout či umožnit poskytnutí Bezpečnostně relevantní dodávky.**

Poddodavatelem je:

orgán či osoba, která **prostřednictvím Přímého dodavatele** Odběrateli **poskytuje či má potenciál poskytnout Bezpečnostně relevantní dodávku.**

Co se týče pojmů, užitých pro vymezení osoby Přímého dodavatele a Poddodavatele, rozumí se *poskytnutím* přímý vývoj, výroba, sestavení či servis produktu (technického vybavení či komunikačního prostředku s výpočetní kapacitou nebo programového vybavení), kdežto *umožněním poskytnutí* pouze prodej, komise či obdobné organizační zajištění takového plnění. *Poskytujícím* tak bude typicky subjekt, který produkt vyrábí, sestavuje či konfiguruje

[7] Ve smyslu § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.

a *umožňujícím poskytnutí* typicky subjekt, který produkt pouze prodává Odběrateli, aniž by sám do produktu zasahoval či jinak napřímo ovlivnil jeho vlastnosti.

S ohledem na principy Mechanismu, uvedené v části 3 Návrhu, usiluje Návrh o stanovení přiměřené hloubky prověřování dodavatelského řetězce. Za tímto účelem vytváří dvě skupiny prověřovaných subjektů, Přímé dodavatele a Poddodavatele. O každé ze skupin prověřovaných subjektů bude vyžadováno různé množství informací, v závislosti na významnosti dané skupiny pro bezpečnost Kritických součástí systému.

Dodavatelský řetězec – přehled změn ve srovnání s Koncepcí:

- **Změna terminologie. „Přímý dodavatel" namísto „Dodavatel 5G sítě". Zaveden je také pojem „poddodavatel" a upuštěno bylo od „prověřovaného subjektu". Revize pojmů byla provedena z důvodu lepšího porozumění, zaměření zůstává stále stejné.**
- **Bezpečnostně relevantní dodávka operuje s nově zavedeným pojmem „kritická součást systému".**
- **Hloubka prověřovaného dodavatelského řetězce je dále předmětem diskusí.**

5 Proces řízení o prověření

S ohledem na obecné zásady a principy procesu rozhodování státu v souvislosti s ochranou nedistributivních práv občanů[8], při němž vznikají či zanikají konkrétní práva a povinnosti osob[9], bude proces posuzování a omezování rizik spojených s Prověřovanými dodavateli správním řízením, vedeným NÚKIB, se speciální právní úpravou v nezbytných aspektech (dále jen „**řízení o prověření**").

Jak je podrobněji popsáno v následujících částech Návrhu, účelem řízení o prověření je posouzení naplnění bezpečnostně relevantních kritérií vztahujících se k osobě Přímého dodavatele a Poddodavatelů ze strany státu. Následkem posouzení naplnění těchto kritérií bude identifikováno případné riziko, spojené s konkrétním dodavatelem, a v návaznosti na toto zjištění bude v řízení rozhodnuto o podmínkách, za jakých je daného dodavatele možné využít pro dodání Bezpečnostně relevantní dodávky.

5.1 Zahájení řízení

Řízení o prověření bude primárně zahájeno na žádost Přímého dodavatele (dále také „**žadatel**"). Náležitostí žádosti o prověření bude předložit ze strany žadatele NÚKIB:

a) žádost o prověření;

[8] Nedistributivními právy občanů jsou ta práva, která jsou nedělitelná a jednotliví občané nemohou být vyloučeni z jejich požívání. Mezi tato práva patří také národní bezpečnost, jejíž ochrana je základním zájmem Mechanismu a důvodem jeho vzniku.

[9] Viz čl. 2 odst. 3 Ústavy České republiky, čl. 2 odst. 2 Listiny základních práv a svobod, § 9 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, aj.

b) prokázání potenciálu dodání Bezpečnostně relevantní dodávky:

   a. prohlášením alespoň jednoho Odběratele, že mu v době podání žádosti žadatel dodává Bezpečnostně relevantní dodávku,

   b. prohlášením alespoň jednoho Odběratele, že od žadatele poptává nebo by případně poptával Bezpečnostně relevantní dodávku nebo

   c. prokázáním splnění podmínek účasti v zadávacím řízení veřejné zakázky, ve kterém bude jednou z podmínek účasti prověření žadatele v řízení o prověření;[10]

c) základní informace o Přímém dodavateli a dle jeho rozhodnutí i o jeho Poddodavatelích.

Žadatel tedy bude žádat o prověření v případě, kdy bude Odběrateli poskytovat nebo zajišťovat poskytnutí Bezpečnostně relevantní dodávky, nebo v případě, kdy bude mít o poskytnutí či zajištění poskytnutí Bezpečnostně relevantní dodávky od žadatele Odběratel zájem. Ačkoliv tedy nebude Odběratel žadatelem (viz část 5.2.1 Návrhu), bude mít na řízení nezanedbatelný nepřímý vliv; obsah rozhodnutí, kterým bude řízení o prověření ukončeno (dále jen „**rozhodnutí o prověření**“, viz část 5.4.1 Návrhu), totiž nesporně ovlivní jeho manažerské rozhodování (viz část 0 Návrhu).

Žádost o prověření bude za celý svůj dodavatelský řetězec podávat Přímý dodavatel, nicméně součástí žádosti budou také informace o jeho Poddodavatelích a rozhodnutí o prověření se bude vztahovat také k těmto osobám. V případě, že bude žadatel – Přímý dodavatel – již disponovat platným rozhodnutím o prověření (viz část 5.4.1 Návrhu), ale některý z jeho Poddodavatelů nikoliv, bude se jím podaná žádost o prověření vztahovat pouze k němu a k těmto dosud neprověřeným Poddodavatelům.

Aby byla zachována efektivita mechanismu (viz část 3 Návrhu), bude povinnou náležitostí žádosti také prokázání žadatelova potenciálu dodání Bezpečnostně relevantní dodávky. Toto prokázání bude moci žadatel splnit buď prohlášením (jakéhokoliv potenciálního) Odběratele, že žadatel poskytuje nebo je schopen poskytnout plnění, které by naplnilo znaky Bezpečnostně relevantní dodávky, anebo samostatným prokázáním splnění obdobných podmínek, které potenciální Odběratel definoval v zadávacích podmínkách veřejné zakázky. Těmito způsoby prokázání by tak měly být omezeny žádosti od žadatelů, kteří nebudou Bezpečnostně relevantní dodávky poskytovat, a zároveň by tak neměl být omezen přístup nových dodavatelů na trh Bezpečnostně relevantních dodávek.

Alternativně k žádosti může být řízení o prověření zahájeno z moci úřední, a to v případě, že se NÚKIB či jiný orgán státní správy zapojený do prověřování dozví o možné změně skutečností, na základě kterých bylo vydáno předchozí rozhodnutí o prověření (viz část 7.3 Návrhu), anebo v případě, že bude v rámci kontroly v oblasti kybernetické bezpečnosti dle § 23 odst. 1 ZKB

[10] Jedinou podmínkou účasti v zadávacím řízení, jejíž splnění nebude muset žadatel společně s žádostí o prověření prokázat, bude přirozeně předchozí prověření žadatele v řízení o prověření; v opačném případě by nebylo možné tímto způsobem potenciál dodání Bezpečnostně relevantní dodávky prokázat.

zjištěno, že je či byla Odběrateli dodávána Bezpečnostně relevantní dodávka od Přímého dodavatele nebo Poddodavatele, který nebyl v řízení o prověření posouzen (viz část 7.4 Návrhu).

Postup po zahájení řízení o prověření bude v obecné rovině odpovídat standardnímu postupu při zahájení správního řízení na žádost či z moci úřední dle § 44 a násl. zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „**SŘ**“).

Zahájení řízení – přehled změn ve srovnání s Koncepcí:

- **Namísto původního zahájení řízení „povinnou osobou Mechanismu“ v Koncepci (nyní Odběratelem) bude o prověření žádat samotný Přímý dodavatel a řízení bude vedeno s ním a s Poddodavateli. Odběratel bude nyní účastníkem řízení pouze v pozici dotčené osoby.**
- **Podmínkou zahájení správního řízení s žadatelem je prokázání potenciálu dodání Bezpečnostně relevantní dodávky.**

5.2 Orgány a osoby zapojené do řízení

5.2.1 Účastníci řízení

Účastníkem řízení o prověření bude především Přímý dodavatel jakožto žadatel, z jehož popudu je řízení o prověření primárně zahájeno a jemuž pro úspěšné vyřízení jeho žádosti náleží povinnost předkládat podklady a sdělovat informace týkající se jeho osoby a Poddodavatelů dané bezpečnostně relevantní dodávky.

Svoji neopominutelnou roli mají v Mechanismu také Odběratelé – kromě pozice dotčené osoby v řízení o prověření totiž definují Bezpečnostně relevantní dodávky, jejichž dodavatelé (Přímí dodavatelé a Poddodavatelé) jsou výhradními prověřovanými subjekty Mechanismu.

I pokud tedy nebudou řízením o prověření práva a povinnosti Odběratele přímo dotčena, bude mít na Odběratele rozhodnutí o prověření nepřímý dopad. Povinností Odběratele bude využívat pro všechny Bezpečnostně relevantní dodávky pouze dodavatele, kteří byli mechanismem prověřeni, a to za podmínek stanovených zákonem a výrokovou částí rozhodnutí o prověření (dopady rozhodnutí o prověření do sféry Odběratele viz v části 0 Návrhu).

V souvislosti s Mechanismem bude Odběratelům pro umožnění analýzy změny okolností, na základě kterých bylo rozhodnutí o prověření vydáno, ze strany NÚKIB také uložena povinnost hlásit NÚKIB Přímé dodavatele a Poddodavatele, kteří jim dodávají Bezpečnostně relevantní dodávky.

5.2.2 Orgány státní správy zapojené do prověřování

Řízení o prověření je vedeno NÚKIB, který tak přijímá žádosti o prověření, koordinuje prověření kritérií prověření (viz část 5.3.2 Návrhu) a vydává rozhodnutí o prověření.

Ostatní orgány státní správy zapojené do prověřování vydávají závazná stanoviska ke splnění či nesplnění jim příslušných kritérií Přímým dodavatelem či poddodavatelem. Dle konkrétního

vymezení kritérií budou orgány státní správy, které budou splnění jednotlivých kritérií vyhodnocovat, určeny podle jejich stávající zákonné působnosti, tak aby příslušný orgán informacemi nezbytnými k vyhodnocení daných kritérií již disponoval nebo aby je byl schopen vyhodnotit s co možná nejmenšími personálními, technickými a finančními náklady.

Lze očekávat, že kromě NÚKIB bude do prověřování zapojeno Ministerstvo vnitra (zejména prostřednictvím Policie České republiky), Ministerstvo průmyslu a obchodu, Ministerstvo financí, Ministerstvo zahraničních věcí a, přiměřeně ke své specifické roli, také zpravodajské služby České republiky. NÚKIB může dále v případě potřeby požádat o informace také další orgány státu, jejichž působnosti se prověřování subjektů týká.

Orgány a osoby zapojené do řízení – přehled změn ve srovnání s Koncepcí:

- **Vzhledem ke změně v osobě žadatele (viz část 5.1 Návrhu) bude účastníkem řízení v této pozici Přímý dodavatel a účastníkem řízení bude spolu s ním také Poddodavatel a Odběratel.**
- **V důsledku bližšího vymezení kritérií prověření (viz část 5.3.2 Návrhu) byl upraven výčet orgánů státní správy zapojených do prověření – byly vyňaty ČTÚ a MPSV jakožto instituce bez věcné působnosti v oblasti kritérií prověření; tyto instituce však mohou být stejně jako další orgány státní správy ČR osloveny ad hoc v případě identifikované potřeby poskytnutí informace.**

5.3 Průběh řízení

Po zahájení správního řízení a případném doplnění nezbytných náležitostí žádosti, budou o zahájení řízení ze strany NÚKIB notifikovány ostatní orgány státní správy zapojené do prověřování (viz část 5.2.2 Návrhu), přičemž jim budou rovněž předány do té doby nashromážděné podklady a informace o Přímém dodavateli a Poddodavatelích. Následně bude započato šetření orgánů státní správy směřující k posouzení naplnění kritérií prověření (viz část 5.3.2 Návrhu), podle jehož výsledku budou Přímý dodavatel a Poddodavatelé zařazeni do příslušné kategorie (viz část 5.3.3 Návrhu) a s využitím jimi dodávaných Bezpečnostně relevantních dodávek Odběratelem budou případně spojena typová opatření (viz část 5.3.4 Návrhu).

Šetření orgánů státní správy směřující k posouzení naplnění kritérií budou probíhat formou závazného stanoviska k řízení o prověření dle § 149 SŘ; v případě zpravodajských služeb nebude vydáno závazné stanovisko, ale budou poskytnuty informace k vyhodnocení naplnění či nenaplnění kritérií prověření.

5.3.1 Sběr informací

Po obdržení notifikace o zahájení řízení zhodnotí orgány státní správy zapojené do prověřování (viz část 5.2.2 Návrhu), zda informace, které mají k dispozici, postačují pro prověření kritérií v jejich působnosti (viz část 5.3.2 Návrhu), nebo zda potřebují od jiného orgánu státní správy či

ze strany Přímého dodavatele nebo Poddodavatele doplnění některých informací nezbytných pro prověření. V případě potřeby doplnění informací pro prověření vyžádá příslušný orgán státní správy tyto informace od jiného správního orgánu nebo prostřednictvím NÚKIB od Přímého dodavatele či Poddodavatele.

5.3.2 Kritéria prověření

Kritéria prověřování budou stanovena s ohledem na cíl Mechanismu omezit strategické bezpečnostní hrozby a rizika spojená s dodavateli, jež Odběratelé nemohou sami prověřit nebo by nebylo přiměřené po nich identifikaci a vyhodnocení takových hrozeb a rizik požadovat.[11] Oblasti, které budou kritéria prověřovat, budou vybrány s ohledem na tento cíl Mechanismu, přičemž budou vycházet z existujících kritérií obdobných systémů, které se zabývají strategickými bezpečnostními hrozbami a jež jsou součástí českého právního řádu[12] a z mezinárodních přístupů k této problematice[13]. Větší rozsah i šíře kritérií budou přitom kladeny na Přímého dodavatele než na Poddodavatele.

Kritéria zkoumající přímo dodavatele budou směřovat k prověření strategických bezpečnostních rizik netechnického charakteru, vycházejících bezprostředně od subjektu dodavatele a z jeho aktivit. Příkladem těchto kritérií mohou být následující:

a) na dodavatele nejsou uvaleny sankce ze strany Evropské unie nebo České republiky;

b) dodavatel nejednal v obchodních vztazích opakovaně v rozporu s pravidly mezinárodního obchodu;

c) dodavatel má transparentní vlastnickou a organizační strukturu;

d) dodavatel má transparentní financování svých podnikatelských aktivit;

e) dodavatel má vlastnickou, organizační či personální vazbu, která umožňuje výkon vlivu na dodavatele vládou či jinou součástí cizího státu.

Kritéria zkoumající stát, do jehož jurisdikce dodavatel spadá či který vykonává nad dodavatelem faktický vliv, budou směřovat k prověření strategických bezpečnostních rizik spojených s motivací a možností cizího státu ovlivnit bezpečnost Kritické součásti systému. Příkladem těchto kritérií mohou být následující:

a) stát je členskou zemí Evropské unie, NATO a jiných nadnárodních a mezinárodních organizací, jejichž členem je Česká republika;

[11] Dle čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, je „zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu“.

[12] Jedná se například o *prověřování zahraničních investic* dle zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic), *prověřování žadatelů o zápis poskytovatele do katalogu cloud computingu* dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů či o *prověřování bezpečnostní způsobilosti* dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

[13] Obdobná kritéria využívají pro účely prověřování rizik spojených s dodavateli Francie, Německo, Estonsko, Nizozemí, Polsko, Švédsko, Finsko a řada dalších evropských i mimoevropských států.

b) stát je demokratickým právním státem, ve kterém je veřejná moc efektivně dělena mezi moc výkonnou, zákonodárnou a soudní;

c) na stát nejsou uvaleny sankce ze strany Evropské unie nebo České republiky nebo stát na Evropskou unii nebo na Českou republiku sám neuvalil sankce;

d) stát opakovaně neporušuje své mezinárodně právní závazky, a to zejména závazky v oblasti lidských práv a mezinárodního obchodu;

e) stát dlouhodobě nejedná proti zájmům Evropské unie, České republiky či jejích spojenců, včetně provádění, financování či jiného podporování kybernetických útoků nebo špionážní či jiné zpravodajské činnosti;

f) stát má s Českou republikou uzavřeny dohody o ochraně nebo spolupráci v oblasti:

   i. bezpečnosti dat (vč. osobních údajů),

   ii. duševního vlastnictví nebo

   iii. kybernetické bezpečnosti,

   anebo se na stát vztahují shodné mezinárodně právní závazky jako na Českou republiku;

g) stát nevyžaduje spolupráci osob ve své jurisdikci pro účely státní bezpečnosti, včetně povinnosti aktivní výměny informací nebo povinného začlenění zástupce státu do organizační struktury dodavatele.

5.3.3 Kategorizace prověřovaných dodavatelů

Jakmile NÚKIB obdrží od zapojených orgánů státní správy výsledky prověření jim příslušných kritérií, s pomocí rozhodovací matice vyhodnotí přítomnost či pravděpodobnost přítomnosti rizika spojeného s Přímým dodavatelem či Poddodavatelem. Dle vyhodnoceného rizika bude příslušný dodavatel označen jako:

A. **dodavatel bez identifikovaného bezpečnostního rizika**, u kterého bylo vyhodnoceno nízké nebo nebylo vyhodnoceno žádné strategické bezpečnostní riziko; u takového dodavatele je narušení bezpečnosti Kritické součásti systému nepravděpodobné;

B. **potenciálně bezpečnostně rizikový dodavatel**, u kterého bylo vyhodnoceno střední strategické bezpečnostní riziko; u takového dodavatele je reálná možnost narušení bezpečnosti Kritické součásti systému;

C. **bezpečnostně rizikový dodavatel**, u kterého bylo vyhodnoceno vysoké strategické riziko; u takového dodavatele je možnost narušení bezpečnosti Kritické součásti systému pravděpodobná až téměř jistá.

5.3.4 Přiřazení opatření

Bude-li Přímý dodavatel či Poddodavatel zařazen do kategorie *dodavatel bez identifikovaného bezpečnostního rizika*, budou Odběratelé moci jeho Bezpečnostně relevantní dodávky využívat bez jakéhokoliv omezení.

V případě, že bude Přímý dodavatel či Poddodavatel zařazen do kategorie *potenciálně bezpečnostně rizikového dodavatele*, budou se k jeho využití pro Bezpečnostně relevantní dodávku pojit typové hrozby a jim příslušná opatření, která budou podmiňovat využití takového dodavatele Odběratelem. Opatření by přitom měla být dostatečně obecná, aby mohla být, s ohledem na stávající systém zavádění bezpečnostních opatření VKB, proveditelně a přiměřeně zavedena do systému Odběratele.

Pakliže bude Přímý dodavatel či Poddodavatel zařazen do kategorie *bezpečnostně rizikový dodavatel*, nebudou Odběratelé moci jeho Bezpečnostně relevantní dodávky využít. Ve výjimečných a odůvodněných případech, zejména pokud se bude jednat o výhradního dodavatele plnění, které je pro Kritickou součást systému nezbytné, bude moci NÚKIB udělit z tohoto pravidla výjimku; žádost o výjimku společně s odůvodněním podá Odběratel a řízení o ní bude samostatným správním řízením, jehož účastníky budou Odběratel a příslušný Přímý dodavatel či Poddodavatel, který byl zařazen do kategorie bezpečnostně rizikového dodavatele.

5.3.5 Lhůty pro prověření

Proces řízení o prověření by měl do vydání rozhodnutí ve věci – rozhodnutí o prověření – proběhnout ve lhůtě do 4 měsíců od zahájení řízení, v případě dobrého informačního zázemí by však mohlo být rozhodnutí o prověření vydáno již za 2 měsíce od řádného podání žádosti o prověření.

Bezodkladně po doručení žádosti o prověření se všemi jejími náležitostmi budou informace o zahájení řízení a související podklady předány ze strany NÚKIB orgánům státní správy zapojeným do prověření a bude započato prověřování příslušných kritérií. Lze očekávat, že časově nejvíce náročnými částmi řízení o prověření bude právě prověřování naplnění kritérií či poskytnutí informací a jejich následné vyhodnocení. Pro vyhodnocení kritérií či poskytnutí informací by proto měly mít zapojené státní orgány v souladu s § 149 odst. 4 SŘ lhůtu jeden až dva měsíce, v závislosti na složitosti prověření v daném případě. Následně by měl mít NÚKIB srovnatelnou lhůtu pro vyhodnocení obdržených informací a přípravu rozhodnutí ve věci, včetně odůvodnění. V závislosti na složitosti případu by tedy mělo standardní řízení o prověření trvat celkově 2 až 4 měsíce.

Skutečnostmi, které mohou standardní délku řízení prodloužit, budou zejména případy přerušení řízení z důvodu nedodání podkladů či neposkytnutí informací žadatelem, potřeba mimořádného došetření informací v souvislosti s potenciálním rizikem či hrozbou spojenou s Přímým dodavatelem či Poddodavatelem či vysoký počet subjektů k prověření v rámci jednoho správního řízení. Celkovou délku řízení může prodloužit také využití opravných prostředků proti vydanému rozhodnutí o prověření. Se speciálním režimem prověření, včetně delších lhůt pro prověření, se počítá bezprostředně po zavedení Mechanismu v rámci přechodných dob.

Průběh řízení – přehled změn ve srovnání s Koncepcí:

- **Byla upřesněna forma stanovisek orgánů státní správy k naplnění kritérií prověření – bude se jednat o závazná stanoviska.**
- **Byla blíže specifikována kritéria prověřování.**
- **Případná možnost eskalace rozhodnutí o prověření není v Návrhu popsána, ale zůstává předmětem diskuse.**

5.4 Ukončení řízení

5.4.1 Vydání rozhodnutí o prověření

Řízení o prověření bude standardně ukončeno vydáním rozhodnutí o prověření, kterým bude určena strategická bezpečnostní rizikovost Přímého dodavatele a Poddodavatelů a případně budou stanovena opatření k omezení identifikovaných rizik či hrozeb anebo omezení využití Přímého dodavatele či Poddodavatele pro bezpečnostně relevantní dodávku.

V případě, že bude v řízení o prověření klasifikován Přímý dodavatel jako *bezpečnostně rizikový dodavatel*, bude se rozhodnutí o prověření vztahovat pouze k jeho osobě, v případě jeho klasifikace jako *potenciálně bezpečnostně rizikového dodavatele* či jako *dodavatele bez identifikovaného bezpečnostního rizika* se pak bude rozhodnutí o prověření vztahovat jak k Přímému dodavateli, tak ke všem Poddodavatelům, které Přímý dodavatel k prověření předložil.

Rozhodnutí o prověření se bude vztahovat vždy ke konkrétnímu dodavatelskému řetězci sestavenému Přímým dodavatelem a bude mít omezenou platnost po dobu 8 let. Po uplynutí doby platnosti rozhodnutí o prověření bude v případě zájmu Přímého dodavatele či Poddodavatele nezbytné projít řízením o prověření opakovaně. Dobu platnosti je nezbytné minimalizovat vzhledem k možné (a v horizontu jednotek let pravděpodobné) změně skutečností, na základě kterých bylo rozhodnutí o prověření vydáno (viz část 7.3 Návrhu), s ohledem na cíl Návrhu minimalizovat dopad Mechanismu na podnikatelské subjekty (viz část 3 Návrhu) však Návrh přichází s variantou, která v maximální možné míře zohledňuje i ekonomickou životnost technologií telekomunikační infrastruktury a investiční horizonty podnikatelských subjektů v sektoru elektronických komunikací.[14] V porovnání s přístupy v zahraničí se jedná o obdobnou či pro soukromý sektor příznivější dobu platnosti podobného rozhodnutí.[15]

[14] NÚKIB při stanovení doby platnosti rozhodnutí o prověření vycházel mimo jiné z informací, které mu o životním cyklu technologií a investičních cyklech v rámci konzultací poskytli samotní zástupci soukromých subjektů v sektoru elektronických komunikací.

[15] Francie uděluje obdobné povolení na maximálně 8 let, Německo uděluje certifikaci jednotlivých kritických prvků infrastruktury dokonce na značně kratší dobu, a to v rozmezí 2 až 5 let.

5.4.2 Přezkum rozhodnutí o prověření

Proti rozhodnutí o prověření se budou za zákonem stanovených podmínek moci účastníci řízení bránit za použití mimořádných opravných prostředků, s výjimkou přezkumného řízení, či případně žalobou ve správním soudnictví.

S ohledem na charakter informací, na jejichž základě budou státem hodnocena kritéria prověření (viz část 5.3.2 Návrhu), které budou mít často povahu utajovaných a případně i zpravodajských informací, jakož i s ohledem na suverénní diskreci státu při hodnocení skutečností, které považuje za bezpečnostní riziko pro svoji kritickou informační infrastrukturu, je nezbytné minimalizovat okruh orgánů a osob, které budou s těmito informacemi seznámeny. Rozhodnutí o prověření z tohoto důvodu nelze přezkoumávat v řízení o rozkladu či v přezkumném řízení, při kterých by k rozšíření okruhu osob, které by se s danými informacemi seznámily, nezbytně došlo. Jelikož však Návrh klade důraz na transparentnost a zákonnost Mechanismu a minimalizaci zásahu do podnikatelského prostředí, ponechává účastníkům řízení o prověření možnost ochrany ve správním soudnictví jakožto pojistky proti případnému nezákonnému postupu státu.

Ukončení řízení – přehled změn ve srovnání s Koncepcí:

- **Byla specifikována doba platnosti rozhodnutí o prověření.**
- **Byly specifikovány možnosti přezkumu rozhodnutí o prověření.**

6 Dopady řízení o prověření na Odběratele

Ačkoliv bude v řízení o prověření rozhodováno o bezpečnostní rizikovosti Přímého dodavatele a Poddodavatelů, bude obsah rozhodnutí o prověření dopadat velkou měrou také na Odběratele.

Povinností Odběratele bude využít pro Bezpečnostně relevantní dodávku pouze Přímého dodavatele a Poddodavatele, který disponuje platným rozhodnutím o prověření, a to za podmínek uvedených ve výroku rozhodnutí. Aby tedy mohl být Odběratelem pro Bezpečnostně relevantní dodávku využit Přímý dodavatel či Poddodavatel, se kterým pojí rozhodnutí o prověření povinnost zavedení opatření nebo jehož využití rozhodnutí o prověření zakazuje, bude muset Odběratel tato opatření zavést, resp. bude muset získat výjimku ze zákazu od NÚKIB (pouze ve výjimečných a odůvodněných případech).

V případě Bezpečnostně relevantní dodávky, která bude trvat nebo která bude přítomná v Kritické součásti systému v době zavedení mechanismu, bude Odběratel povinen informovat Přímé dodavatele a Poddodavatele o vzniku povinnosti prověření a dle obsahu následného rozhodnutí o prověření bude Odběratel případně povinen tak zavést dodatečná opatření nebo Přímého dodavatele či Poddodavatele, klasifikovaného jako bezpečnostně rizikového dodavatele, z Bezpečnostně relevantní dodávky vyloučit. V případě takto založené povinnosti

bude mít ovšem Odběratel možnost využít přechodné lhůty (viz část 7. 2 Návrhu) k zavedení opatření či k vyloučení identifikovaných *bezpečnostně rizikových dodavatelů*.

Dopady řízení o prověření na Odběratele – změny oproti Koncepci:

- **Nová kapitola, vzniklá v důsledku podrobnější struktury Návrhu oproti Koncepci.**

7 Další aspekty Mechanismu

7.1 Evidence prověřených dodavatelů

K řízení o prověřování bude vedena příslušná spisová agenda, jejíž součástí budou zejména podané žádosti o prověření, podklady k prověření a rozhodnutí o prověření, a tedy i evidence prověřených Přímých dodavatelů a Poddodavatelů; některé části spisové agendy, například informace k prověření poskytnuté zpravodajskými službami, budou s ohledem na jejich citlivost a možný dopad na bezpečnost České republiky vedeny v utajovaném režimu.

Orgány státní správy budou mít díky přístupu k evidenci prověřovaných dodavatelů v případě opakovaného prověření možnost zhodnotit kritéria prověřování s pomocí informací z předchozích řízení o prověření a tím provést prověření v souladu s principem efektivity Návrhu (viz část 3 Návrhu) rychleji a s vynaložením minimálních nezbytných nákladů. Evidence prověřených dodavatelů bude sloužit rovněž k prověření změny skutečností, na jejichž základě bylo vydáno předchozí rozhodnutí o prověření, a případnému zahájení nového řízení o prověření z moci úřední (viz část 5.1 Návrhu).

7.2 Prověření stávajících dodavatelů

Po zavedení Mechanismu do praxe bude v rámci přechodných ustanovení právního předpisu, kterým bude Mechanismus zaveden, uložena povinnost prověření také Přímých dodavatelů a Poddodavatelů Bezpečnostně relevantních dodávek, které budou v okamžiku zavedení Mechanismu trvat nebo budou přítomné v Kritické součásti systému.

V přiměřené době po zavedení Mechanismu tak bude Odběratel povinen informovat Přímého dodavatele o skutečnosti, že dodává Bezpečnostně relevantní dodávku a že se na něj a na jeho Poddodavatele nově vztahuje povinnost prověření. Bez zbytečného odkladu poté bude Přímý dodavatel povinen zažádat o prověření.

Na rozdíl od standardního prověření nebude v případě řízení o prověření po zavedení Mechanismu vyžadováno bezprostřední zavedení opatření ke zmírnění identifikovaného rizika spojeného s dodavatelem či vyloučení dodavatele z Bezpečnostně relevantní dodávky. Opatření či povinnost vyloučení budou uloženy s povinností jejich zavedení do 5 let od nabytí právní moci rozhodnutí o prověření. Tuto mimořádnou lhůtu k provedení opatření představuje Návrh jako jednu z variant přístupu k přechodnému období po zavedení mechanismu, která je vstřícná k Odběratelům, kteří před zavedením mechanismu nebudou mít nebo budou mít pouze

omezenou znalost bezpečnostní rizikovosti jejich dodavatelů. Délka lhůty byla stanovena tak, aby poskytovala Odběratelům dostatečný prostor pro zajištění Bezpečnostně relevantních dodávek pouze od dodavatelů prověřených Mechanismem a pro zavedení případných opatření uložených rozhodnutím o prověření; v praxi bude lhůta pro zajištění souladu Odběratele s Mechanismem prodloužena ještě o legisvakanci. V porovnání s přístupy v zahraničí se jedná o obdobnou či pro soukromý sektor příznivější lhůtu pro zajištění souladu.[16]

7.3 Opakované řízení o prověření

Přímí dodavatelé a Poddodavatelé budou opakovaně prověřování primárně na žádost v případě uplynutí platnosti rozhodnutí o prověření, které se jich týká (viz část 5.4.1 Návrhu).

Opakované řízení o prověření bude zahajováno též z moci úřední, a to v případě změny skutečností, na základě kterých bylo vydáno předchozí rozhodnutí o prověření, nebo v případě, že bude v rámci kontroly v oblasti kybernetické bezpečnosti zjištěno, že je či byla Odběrateli dodávána Bezpečnostně relevantní dodávka od Poddodavatele, který nebyl v předchozím řízení o prověření posouzen (viz část 7.4 Návrhu). Za účelem zahájení řízení následkem změny skutečností, na základě kterých bylo rozhodnutí o prověření vydáno, bude mít Přímý dodavatel povinnost oznámit NÚKIB změnu jakékoliv z konkrétně vymezených skutečností, vztahující se k jeho osobě nebo k osobě některého z jeho Poddodavatelů.

Příkladem skutečností, jejichž změna bude NÚKIB povinně oznamována je:

a) změna sídla Přímého dodavatele nebo Poddodavatele či jejich ovládajících osob[17];

b) změna v ovládající osobě Přímého dodavatele nebo Poddodavatele[18].

Pokud bude na žádost vydáno opakované rozhodnutí o prověření, zatímco předchozí rozhodnutí o prověření bude stále platné, budou se do skončení platnosti původního rozhodnutí o prověření aplikovat přiřazená opatření (viz části 5.3.4 a 0 Návrhu) z tohoto rozhodnutí, s výjimkou případů, kdy nové rozhodnutí o prověření zařadí Přímého dodavatele či Poddodavatele do méně rizikové kategorie (viz část 5.3.3 Návrhu). Účelem tohoto procesu je minimalizace zátěže Mechanismu pro Odběratele a maximalizace předvídatelnosti povinností uložených rozhodnutím o prověření – po dobu platnosti již případně zavedených opatření totiž nebudou ve vztahu ke konkrétním osobám zaváděna nová opatření, ale mohou být pouze omezena ta stávající.

Pro podrobný popis podmínek zahájení opakovaného řízení o prověření viz část 5.1 Návrhu.

7.4 Kontrola

Dodržování povinností uložených Mechanismem bude kontrolováno NÚKIB v rámci kontroly v oblasti kybernetické bezpečnosti dle § 23 odst. 1 ZKB. Bude-li tedy při kontrole NÚKIB zjištěno,

[16] V zahraničí jsou obdobné lhůty stanoveny zpravidla v rozmezí 4 až 7 let; např. Spojené království a Německo mají přechodné lhůty stanovené na 5 let.

[17] Ve smyslu § 74 odst. 1 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.

[18] S ohledem na maximální využití již existujících zákonných mechanismů je vhodné obdobně využít například § 4 zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).

že Odběratel využívá pro Bezpečnostně relevantní dodávku Přímého dodavatele či Poddodavatele, který nedisponuje platným rozhodnutím o prověření, nebo že Odběratel pro Kritickou součást systému nezohlednil obsah rozhodnutí o prověření, může být Odběrateli uložena sankce a nápravná opatření dle § 24 ZKB (zpravidla povinnost zavedení opatření dle rozhodnutí o prověření nebo vyloučení předmětného Přímého dodavatele či Poddodavatele z Bezpečnostně relevantní dodávky).

7.5 Metodická podpora

V souladu s dlouhodobou praxí NÚKIB bude všem orgánům a osobám, kterým budou Mechanismem ukládána práva a povinnosti, jakož i jiným Mechanismem dotčeným subjektům, poskytována metodická podpora a pomoc, a to jak na individuální bázi, tak formou obecných metodických pokynů a doporučení.

7 Další aspekty Mechanismu – přehled změn oproti Koncepci:

- **Doplněn popis okolností opakování řízení o prověření.**

8 Závěr

Návrh rozpracovává Koncepci za účelem konzultace a diskuse o podobě nové regulace v oblasti kybernetické bezpečnosti elektronických komunikací v rámci státního a soukromého sektoru. Vychází přitom jak ze samotné Koncepce, tak z příkladů dobré praxe obdobné zahraniční regulace a z vyjádření zástupců soukromého sektoru v oblasti elektronických komunikací a diskuse těchto zástupců s NÚKIB a spolupředkladateli budoucího návrhu věcného záměru zákona (viz část 1 Návrhu).

Zvolená míra rozpracování Návrhu umožňuje utvoření si základního přehledu o možné podobě Mechanismu, aniž by zacházel do přílišných podrobností a znemožňoval tak koncepční uvažování o celém navrhovaném řešení.

Cílem Návrhu přitom není představení závazného výsledného řešení, ale podnícení diskuse o vhodných podobách řešení z pohledu jak státního, tak soukromého sektoru, které by Návrh dále modifikovaly až do podoby věcného záměru zákona. Kromě návrhů na výslednou podobu Mechanismu uvítá NÚKIB také jakoukoliv konstruktivní zpětnou vazbu k agendě kybernetické bezpečnosti dodavatelského řetězce obecně, jakož i k ostatním agendám, kterými se NÚKIB zabývá, a k vzájemné spolupráci s NÚKIB jako takové.

9 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	**Podmínky použití**
Červená 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.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
Zelená 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.
Bílá TLP: (WHITE)	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.