25. 8. 2020

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

Zpráva o pokroku členských států v implementaci EU Toolbox: Jak přistupovat k rizikovým dodavatelům?

Skupina pro spolupráci EU dne 24. 7. 2020 zveřejnila dokument nazvaný „Zpráva o pokroku členských států v implementaci EU Toolbox".[1] Dokument přináší nejen informace o stavu implementace a jejím časovém plánu, ale i příklady konkrétních opatření, která vybrané členské státy v oblasti zajištění bezpečnosti 5G sítí přijaly. A některá z nich mohou být inspirací i pro ČR.

Skupina pro spolupráci EU vydala dne 29. ledna 2020 *„Soubor opatření EU pro kybernetickou bezpečnost sítí 5G"*[2], neboli EU Toolbox. Ten jednotlivým členským státům předkládá, jaká opatření by měla být přijata na úseku kybernetické bezpečnosti. EU Toolbox má zajistit na evropské úrovni jednotný koordinovaný přístup, založený na sadě opatření zaměřených na zmírnění hlavních kybernetických bezpečnostních rizik sítí páté generace. Konečným cílem je vytvořit spolehlivý rámec bezpečnostních opatření, který zajistí odpovídající úroveň kybernetické bezpečnosti sítí 5G v celé EU prostřednictvím účinných koordinovaných přístupů.

EU Toolbox definuje tři skupiny opatření, která dělí na strategická, technická a podpůrná. Zpráva o pokroku členských států v implementaci EU Toolbox (dále jen *„Zpráva o implementaci"*) detailně pojednává o stavu implementace jednotlivých strategických a technických opatření. Jedním z rozebíraných opatření je i strategické opatření SM03: Posouzení rizikového profilu dodavatelů a uplatňování omezení u dodavatelů považovaných za vysoce rizikové – včetně nezbytných vyloučení pro účinné zmírnění rizik – pro klíčová aktiva. To je zásadní i z pohledu současných diskuzí o tom, kteří dodavatelé (resp. na základě jakých kritérií) by měli být k budování 5G sítí připuštěni. Co tedy Zpráva o implementaci o přístupu členských států EU k rizikovým dodavatelům uvádí?

Zpráva o implementaci k uvedenému opatření obecně shrnuje: *„Několik členských států již implementovalo opatření zaměřená na minimalizaci vystavení rizikům ze strany dodavatelů považovaných za vysoce rizikové, zatímco ve velké většině ostatních členských států tento proces stále probíhá a v mnoha případech již dobře pokročil. Malá menšina členských států nesdělila konkrétní informace o svých plánech na implementaci tohoto opatření.*

U těch, kde proces ještě nebyl zahájen nebo dokončen, však často chybí jasné informace o časovém rámci pro implementaci tohoto opatření. To může souviset se složitostí a citlivostí tohoto opatření, které vyžaduje zohlednění širšího spektra faktorů, zejména netechnických faktorů (např. riziko zásahů ze strany třetí země), jakož i potenciálních nákladů specifických pro daný sektor a širších ekonomických nebo společenských dopadů."[3]

Samotná Zpráva o implementaci zdůrazňuje citlivost opatření a netechnické faktory (mající do značné míry politický charakter), které mají být při posuzování rizikovosti dodavatele vzaty v úvahu. Zpráva o implementaci rovněž doplňuje dva faktory, které mají být pro účinnou implementaci strategického opatření SM03 zásadní. Jedním je metodika používaná k posouzení rizikového profilu dodavatelů, druhým pak definice klíčových aktiv, na která se budou vztahovat omezení.

Zpráva o implementaci dále popisuje různé přístupy členských států k rizikovým dodavatelům. Ty shrnuje následujícím způsobem:

- Předchozí schválení nebo notifikace/veto: Posouzení plánů operátorů a uložení omezení nebo vyloučení případ od případu, s přihlédnutím k řadě aspektů, včetně charakteristik jednotlivých dodavatelů a specifických způsobů zavádění; tento přístup obvykle nezahrnuje systematická nebo blanketní opatření týkající se konkrétního dodavatele;
- „Deny list“: Určení určitých dodavatelů jako vysoce rizikové nebo nedůvěryhodné a na tomto základě uplatnění omezení nebo zákazů pro operátory, aby z nich získávali určité zařízení nebo služby; uvažovaná omezení mohou mít formu vyloučení nebo omezení a/nebo limitu podílu dodavatele (dodavatelů) v sítích;
- „Allow list“: Identifikace konkrétních dodavatelů, kteří by mohli dodávat zařízení či služby pro 5G sítě.

Zpráva o implementaci dále předkládá stručný popis přístupů vybraných členských států, konkrétně (i) Francie, kde jsou nařízením definována klíčová síťová aktiva, přičemž tato podléhající kontrole a schválení před jejich zavedením, (ii) Itálie, kde má vláda právo možnost vetovat smlouvu či uložit určitá bezpečnostní opatření v případě použití zařízení nebo služeb od provozovatelů mobilních sítí k rozmístění 5G, kdykoli je toto zařízení nebo služba získáno od dodavatelů mimo EU a (iii) Nizozemsko, kde jsou stanovena kritéria, na jejichž základě budou jmenováni nedůvěryhodní dodavatelé.

Z uvedeného je zřejmé, že přístup jednotlivých členských států je různý. ČR dosud konkrétní přístup k rizikovým dodavatelům nevytvořila. Volba řešení je i s ohledem na doporučující charakter EU Toolboxu na vnitrostátním uvážení. Avšak může být přínosné při tvorbě podmínek vzít v úvahu přístupy zvolené v ostatních členských státech.

Jako jeden z nich lze zmínit i nedávno zveřejněný[4] koncept německého řešení. To v zásadě spočívá ve dvou fázích, kdy v první je rozhodováno o připuštění dodavatele k budování 5G sítí na základě objektivních technických kritérií. I v případě jejich splnění si stát stále ponechá možnost příslušného dodavatele vyloučit. K tomu by však mělo docházet zřejmě spíše výjimečně, a to pokud se pro takový postup vyjádří jednomyslně Úřad spolkového kancléře, Úřad pro zahraniční věci, Ministerstvo vnitra a Ministerstvo průmyslu.

Koncepčně lze popsaný přístup považovat za určitý kompromis zajišťující jak ochranu bezpečnostních zájmů státu, tak i efektivní budování 5G sítí bez nepřiměřeného omezení volné hospodářské soutěže. Lze si jej tak představit i v českých podmínkách. I zde by tedy stát primárně rozhodoval na základě objektivních kritérií, která by byla stejná pro všechny dodavatele. Pokud by měla být státu ponechána možnost vyloučení dodavatele, který testem objektivních kritérií úspěšně prošel, mělo by se jednat o zcela výjimečnou možnost, kdy podmínky takového (svojí povahou zpravidla politického) rozhodnutí by byly předem jasně stanoveny.

Mgr. Petr Motyčka,
advokát

založeno 1990
TOMAN & PARTNEŘI
ADVOKÁTNÍ KANCELÁŘ
www.iustitia.cz
PARTNER PRO VÁŠ PRACOVNÍ I OSOBNÍ ŽIVOT

TOMAN & PARTNEŘI advokátní kancelář, s.r.o.

Trojanova 12
120 00 Praha 2

Tel.: +420 224 918 490
Fax: +420 224 920 468
e-mail: ak@iustitia.cz

---

[1] „Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity", k dispozici >>> zde.

[2] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, k dispozici >>> zde.

[3] Zpráva o implementaci není oficiálně dostupná v českém jazyce. Citace představují překlad autora článku.

[4] Viz např. k dispozici >>> zde.

Další články:

- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- TOP 5 judikátů z korporátního práva za rok 2025
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Proč dnes více než polovina M&A transakcí ve střední Evropě nekončí podpisem
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Návrh nového zákona o digitální ekonomice
- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách