Národní úřad pro kybernetickou bezpečnost

K rukám Mgr. Petra Novotného

Ředitele odboru kybernetických bezpečnostních politik

Mučednická 1125/31

616 00 Brno

Praha, 7. dubna 2022

# Připomínky Asociace provozovatelů mobilních sítí (APMS) k dokumentu „Návrh mechanismu posuzování a omezování rizik spojených s dodavateli do infrastruktury elektronických komunikací“

1. Tento dokument navazuje na dřívější připomínky Asociace provozovatelů mobilních sítí („**APMS**“) k záměru Národního úřad pro informační a kybernetickou bezpečnost („**NÚKIB**“) regulovat svobodu provozovatelů sítí elektronických komunikací volit dodavatele síťové a další infrastruktury. Odkazujeme se proto zejména na náš dopis adresovaný NUKIB ze dne 23. 2. 2022. S obsahem těchto vyjádření se nadále plně ztotožňujeme, považujeme je za relevantní a žádáme NÚKIB o jejich zohlednění při další práci na návrhu Mechanismu posuzování a omezování rizik spojených s dodavateli do infrastruktury elektronických komunikací („**Mechanismus**“)
2. S ohledem na to, že Mechanismus bude zasahovat do práva na podnikání garantovaného čl. 26 odst. 1 Listiny základních práv a svobod („**LZPS**“), je nezbytné, aby NÚKIB záměry Mechanismu dostatečně odůvodnil a vysvětlil, jaký jiný chráněný zájem staví na roveň svobody podnikatelských subjektů své základní právo realizovat. Toto odůvodnění však návrh Mechanismu postrádá.
3. Návrh Mechanismu je v rozporu s Programovým prohlášením vlády České republiky[[1]](#footnote-1), které se v části „Vnitřní bezpečnost a veřejná správa“ zabývá zjednodušováním povinností podnikatelů vůči státu. Návrh Mechanismu také nevysvětluje návaznost na kapitolu „Digitalizace“ v části „Kybernetická bezpečnost“, když se namísto koordinovaného přístupu jeví být jednostranným postupem NÚKIB bez vazby na skutečné hrozby i v jiných odvětvích, než jsou elektronické komunikace. V neposlední řadě pak návrh Mechanismu ohrožuje naplnění kapitoly „Digitalizace“ v části „Konektivita a rozvoj sítí“, když ohrožuje flexibilní a stabilní technologický rozvoj a interoperabilitu v důsledku netransparentního hodnotícího procesu dle návrhu Mechanismu.
4. V návrhu Mechanismu stále zcela chybí jakákoli, byť jen počáteční analýza dopadů na podnikatelské prostředí v oboru elektronických komunikací, po které voláme již od začátku. Není možné nejdříve připravovat mechanismus a pak nalézat důvody, proč je třeba právě taková podoba mechanismu, kterou NÚKIB preferuje. Je potřeba nejprve analyzovat, jaký je stav v oblasti dodávek do jednotlivých částí sítě a poté v souladu se zásadou proporcionality vybrat takovou formu regulace, která splní požadavky zákonodárce s co nejmenšími dopady na volný trh a svobodu podnikání. Opět si dovolíme odkázat se na programové prohlášení vlády, které uvádí: „*Zvýšíme kvalitu legislativy. Každou novou regulaci důkladně zvážíme na základě analýzy očekávaných dopadů. Legislativní návrhy potřebné k plnění programového prohlášení budou předkládány standardní legislativní cestou a před jejich předložením do vlády se k nim vyjádří odborníci v rámci Legislativní rady vlády*.“
5. Je nepochybné, že případná implementace a provádění Mechanismu (tak jak je aktuálně navrhován) by měla významný dopad na rozvoj, rozšiřování a zkvalitňování digitální komunikační infrastruktury v České republice. Provozovatelé sítí elektronických komunikací, kteří budou předmětem procesů definovaných Mechanismem, budou postiženy významnou mírou nejistoty ohledně svých budoucích investic. Pokud nebude navržen a v praxi zajištěn mitigační proces pro nutné zvýšené investiční náklady v přechodném období implementace Mechanismu, je velmi pravděpodobné, že plánované investice do nových či modernizovaných sítí elektronických (a to jak mobilních, tak pevných) budou omezeny či zpožděny a bude nutné soukromé investice upřednostnit v oblastech vedoucích k naplnění povinností či očekávání spojených s Mechanismem. Jsme přesvědčeni, že Mechanismus, tak jak je navržen, může vést ke zpoždění rozvoje a modernizace pevných a mobilních (zejména těch ve standardu 5G) sítí s vysokou kapacitou (tzv. VHCN sítí) a k menšímu rozvoji těchto sítí ve venkovských oblastech, resp. v oblastech s menší návratností investice. Může dojít k tomu, že Česká republika k roku 2030 nesplní cíle Digitální dekády[[2]](#footnote-2). Bude též nutné přehodnotit povinnosti (zejména povinnosti dosažení pokrytí) vyplývající z přídělů kmitočtů získaných ve výběrovém řízení (aukci) na kmitočty 5G uskutečněné v roce 2020.
6. Vzhledem k nedostatku citovanému v odst. 2, stejně jako k dalším nedostatkům citovaným dále v tomto dokumentu, považuje APMS poskytnutou lhůtu k připomínkování v délce trvání tří týdnů za nedostačující a vyzývá NÚKIB, aby po nápravě nedostatků přistoupil ke konzultaci nové v délce trvání nejméně jednoho měsíce. APMS se neztotožňuje s argumentem NÚKIB citovaným v dopise ze dne 29. března 2022, Č. j.: 3730/2022-NÚKIB-E/310, že s ohledem na plán přípravy věcného záměru zákona do konce kalendářního roku 2022 není možné poskytnout ke konzultaci lhůtu delší; nedostatečné plánování času potřebného pro přípravu věcného záměru Mechanismu nemůže NÚKIB klást k tíži podnikatelského sektoru, který má v úmyslu regulovat a jehož základní práva a svobody zamýšlí omezit.
7. Zdá se, že návrh Mechanismu rozšiřuje dosavadní cílovou skupinu subjektů a objektů nad rámec technologie 5G, aniž by vysvětlil, z jakého důvodu tomu tak je. APMS nadále rozporuje potřebu specifického přístupu k sítím elektronických komunikací odlišného od jiných systémů a prvků kritické, resp. kritické informační infrastruktury. S ohledem na to, že NÚKIB dosud uspokojivě nedoložil přezkoumatelnými argumenty potřebu regulace technologie 5G, není proto srozumitelné ani přezkoumatelné, proč v návrhu Mechanismu rozšiřuje svůj záběr dále i na další, blíže nespecifikované, technologie. Postup NÚKIB je tak nejméně na hraně zvůle správního orgánu.
8. Stejně jako v předchozích dokumentech NÚKIB ani v návrhu Mechanismu nerozlišuje mezi softwarovými a hardwarovými prvky. Nelze akceptovat, že správní orgán v oblasti kybernetické bezpečnosti vůbec nezohlednil specifika pravidelných updatů a upgradů softwarových, resp. firmwarových komponent a stanovil obecně přezkumnou proceduru bez ohledu na to, že k softwarových, resp. firmwarovým, úpravám zkoumaných systémů dochází až několikrát denně. Jakákoli přezkumná činnost NÚKIB tak postrádá logiku a sama se tak ukazuje jako bezvýsledná a zbytečná bez reálného dopadu na skutečný stav kybernetické bezpečnosti.
9. Ze strany telekomunikačního sektoru jsme opakovaně upozorňovali na náklady, jež vzniknou v důsledku nové regulace navrhované v Mechanismu. Této odpovědnosti se NÚKIB nemůže zbavit ani konstatováním, že upozorňuje na rizika, když (i) regulace vznikne až po vynaložení nákladů, (ii) parametry posuzování jsou stále nejasné a netransparentní, (iii) návrh Mechanismu je zcela nekonkrétní, a (iv) ze strany orgánu veřejné moci dojde do svévolného zásahu do soukromé sféry podnikatele.
10. Obecnost, netransparentnost a nepřezkoumatelnost jak návrhu Mechanismu, tak správního řízení, které z něj má dle textu návrhu Mechanismu vycházet, podporují korupční prostředí. Je to dáno zejména chybějícími jednoznačnými parametry a výslovně deklarovanou nepřezkoumatelností rozhodnutí NÚKIB.
11. NÚKIB se v návrhu Mechanismu odklání od dokumentů, na jejichž tvorbě se sám podílel, jako je např. přístup koordinovaného posouzení rizik kybernetické bezpečnosti v 5G sítích (EU coordinated risk assessment of the cybersecurity of 5G networks) a Souboru opatření EU pro bezpečnost sítí 5G (EU 5G Toolbox). To je v rozporu s Usnesením Bezpečnostní rady státu ze dne 19. října 2021 č. 33, podle kterého bylo právě naplnění opatření SM03 Souboru opatření EU pro kybernetickou bezpečnost sítí 5G cílem celého Mechanismu.
12. Návrh Mechanismu postrádá vysvětlení nezbytných rozdílných přístupů regulátorů v různých zemích zavádějících podobný režim regulace. Jak bude NÚKIB řešit situaci, kdy centralizovaná řešení zahrnující propojené osoby ve více zemích budou moci užívat zařízení od dodavatelů, které se nebudou ze strany NÚKIB schváleni, resp. jak bude NÚKIB obecně řešit neshodu mezi různými regulátory v různých zemích? Bude v takovém případě muset tuzemský subjekt používat zařízení od jiného dodavatele a znemožnit tak infrastrukturní propojení mezi propojenými subjekty? Jak bude přistupovat NÚKIB k evropským prvkům kritické informační infrastruktury? NÚKIB do definice kritické informační infrastruktury zahrnuje také fyzické osoby (zaměstnance apod.). Znamená to, že bude NÚKIB prověřovat fyzické osoby dodavatelů jako jsou dodavatelé údržby, instalační technici a například pracovníci ostrahy na infrastrukturním centru v zahraničí, které tuzemský provozovatel prvku kritické informační infrastruktury používá? Žádáme NÚKIB o vysvětlení.
13. Realizace Mechanismu povede k omezení hospodářské soutěže na trhu nabídky komponent infrastruktury sítí elektronických komunikací. Pokud jeden ze tří v současnosti využívaných dodavatelů (Nokia, Ericsson, Huawei) nebude smět dodávat do České republiky prvky infrastruktury pro sítě elektronických komunikací, znamená to podporu duopolu dodavatelů, růst cen komponent, omezení jejich dostupnosti a rozvrat infrastruktury sítí elektronických komunikací, když jednotlivé prvky od různých dodavatelů nelze kombinovat. Máme dále pochybnost o udržitelnosti tohoto stavu v situaci, kdy společnost Ericsson je vyšetřována pro spolupráci s Islámským státem[[3]](#footnote-3) a společnost Nokia se podílela na budování infrastruktury využívané ruskou službou FSB[[4]](#footnote-4). Bude NÚKIB garantovat budoucí možnost odebírat prvky infrastruktury sítí elektronických komunikací od těchto dodavatelů, nebo se může stát, že zakáže i je, jako se to stalo v Rumunsku společnosti Nokia[[5]](#footnote-5)? Žádáme NÚKIB o vysvětlení.
14. **Komentáře ke kapitole 3 návrhu Mechanismu:**
	1. V úvodním odstavci návrh Mechanismu používá pojem „strategicky významná komunikační infrastruktura, aniž by jej dále vysvětloval, resp. aniž by bylo zřejmé, jakou infrastrukturu považuje za *strategicky významnou* a jakou za *strategicky nevýznamnou*. Bez dostatečného vysvětlení tohoto základního pojmu je zbytek návrhu Mechanismu zbytečný, neboť postrádá základní ukotvení. Žádáme NÚKIB o vysvětlení.
	2. Rozporujeme prohlášení z úvodního odstavce, že infrastruktura sítí 5G spadá do regulace zákona č. 181/2014 Sb., o kybernetické bezpečnosti („**ZKB**“), když ZKB takový princip nezakotvuje a není ani zřejmé, na základě čeho, NÚKIB dospěl k závěru, že právě sítě 5G mají zvláštní postavení a měly by zcela spadat do režimu ZKB. Žádáme NÚKIB o vysvětlení.
	3. Rozporujeme prohlášení z druhého odstavce o významu regulace „důležité infrastruktury státu“, neboť návrh Mechanismu vysvětlení tohoto pojmu neobsahuje a není zřejmé, jaký význam mu NÚKIB přikládá. Bez dostatečného vysvětlení tohoto základního pojmu je zbytek návrhu Mechanismu zbytečný, neboť postrádá základní ukotvení. Žádáme NÚKIB o vysvětlení.
	4. NÚKIB v první odrážce na str. 5 odkazuje na „existující riziko ingerence státních aktérů do produktů, služeb či procesů prostřednictvím dodavatelů či poddodavatelů, s cílem narušení bezpečnosti (včetně dostupnosti) strategické informační a komunikační infrastruktury státu“, aniž by dále specifikoval, co tímto pojmem má na mysli a jaké hrozby pod tento pojem zahrnuje. Pro úplnost připomínáme, že nám není znám stát původu technologií ICT, který by nebyl v nedávné minulosti zapojen do činnosti narušující národní suverenitu států EU, a to včetně Spojených států amerických[[6]](#footnote-6). Bez dostatečného vysvětlení tohoto základního pojmu je zbytek návrhu Mechanismu zbytečný, neboť postrádá základní ukotvení. Žádáme NÚKIB o upřesnění, které státní aktéry považuje za bezpečné a které za rizikové a na základě jakých kritérií relevantních pro výběr dodavatelů sítí elektronických komunikací.
	5. Žádáme o vysvětlení významu druhé odrážky na straně 5, když tam popsané principy jsou již dnes regulovány ZKB.
	6. Návrh Mechanismu a jeho důsledku pro soukromý sektor musí nezbytně vézt ke zvýšení nákladů oproti stávajícímu stavu. Vycházíme ze základní premisy, že zájmem podnikatelů je generovat zisk kombinací maximalizace výnosů a minimalizace nákladů. S ohledem na to, že se NÚKIB chystá regulatorně do tohoto stavu zasáhnout, je nezbytným důsledkem růst nákladů na straně podnikatelů. Žádáme NÚKIB o vysvětlení, proč považuje zásah do podnikání provozovatelů sítí elektronických komunikací za nezbytný a jaký test proporcionality k tomu NÚKIB vypracoval.
15. **Komentáře ke kapitole 4 návrhu Mechanismu:**
	1. V podkapitole 4.2 návrhu Mechanismu se uvádí, že součástí systému podléhající Mechanismu mají být „technická aktiva“, tedy „technické vybavení, komunikační prostředky a programové vybavení, na jejichž správném a spolehlivém fungování je závislé připojení kritické informační infrastruktury k síti elektronických komunikací“. Dále se v téže podkapitole rozvádí, že „[P]ředmětem prověřování Mechanismem jsou […] všechna technická aktiva, na nichž je připojení [kritické infrastruktury] závislé z pohledu inherentních rizik“. Považujeme takové vysvětlení za zcela nedostatečné (i) protože pojem „připojení kritické infrastruktury“ může zahrnovat prakticky jakýkoli prvek a návrh Mechanismu nepracuje se skutečnou logikou architektury sítí elektronických komunikací, ale pouze s obecným prohlášením, pro něž není legislativní ani jiné opory, a dále (ii) protože neposkytuje vodítko pro pojem „inherentní riziko“ a tím neumožňuje posoudit relevantnost návrhu v podkapitole 4.2. Žádáme NÚKIB o vysvětlení.
	2. V podkapitole 4.3.1 definuje návrh Mechanismu „bezpečnostně relevantní dodávku“ tak široce, že může zahrnovat prakticky jakýkoli prvek dotýkající se jakkoli *Kritické součásti systému*. NÚKIB je z jeho činnosti jistě známa šíře prvků a systémů používaných při zajišťování činnosti sítí elektronických komunikací. Proto je namístě, aby tuto zkušenost využil zúžením rozsahu definice pojmu „bezpečnostně relevantní dodávka“ tak, aby z něj byl zřejmý chráněný zájem a jeho interpretace tak byla postavena najisto. Žádáme NÚKIB o zpřesnění.
	3. V podkapitole 4.3.2 návrhu Mechanismu je definice „prověřovaného dodavatele“ natolik široká, že zahrnuje celé podnikatelské seskupení, tj. včetně zahraničních propojených subjektů mimo jurisdikci NÚKIB. Tento pojem je tak neinterpretovatelný. Totéž platí, možná ještě ve větší míře pro pojem „poddodavatel“, kterým je v pojetí NÚKIB mj. subjekt, který „má potenciál“ (sic!) poskytnout bezpečnostně relevantní dodávku. NÚKIB tak *de facto* rozšiřuje dopad Mechanismu na jakéhokoli dodavatele v oboru ICT, což nelze akceptovat, neboť tím NÚKIB zcela vybočuje ze své působnosti[[7]](#footnote-7), ale také proto, že tím popírá sám své vlastní principy efektivity stanovené v úvodu návrhu Mechanismu. Žádáme NÚKIB o opravu a zpřesnění.
16. **Komentáře ke kapitole 5 návrhu Mechanismu:**
	1. Již podkapitola 5.1 obsahuje závažný zásah do povinnosti statutárního orgánu jednat s péčí řádného hospodáře[[8]](#footnote-8), když možnost rozhodnout o relevantních skutečnostech v kontextu svého podnikání na sebe přebírá NÚKIB. To je patrné například v části posuzování „žadatelova potenciálu dodání Bezpečnostně relevantní dodávky“. Návrh Mechanismu sice uvádí možnost prokázání prohlášením Odběratele, avšak z kontextu je zřejmé, že tuto skutečnost zamýšlí NÚKIB přezkoumávat (jinak by takové důkazy ve správním řízení požadovat nemohl[[9]](#footnote-9)). Nejenže tak NÚKIB zamýšlí netransparentně zasáhnout do práv podnikatelů, ale přejímá na sebe odpovědnost za způsobilost dodavatele dodat Bezpečnostně relevantní dodávku včetně odpovědnosti za škodu vzniklou porušením tohoto prohlášení dodavatele. Žádáme NÚKIB o vysvětlení.
	2. Již dříve jsme upozorňovali na časovou kritičnost procesu s ohledem na nezbytnost zachování provozuschopnosti prvků a systémů kritické informační infrastruktury a kritické infrastruktury. Navzdory tomu NÚKIB ani v tomto návrhu Mechanismu stále nestanovil jednoznačnou lhůtu pro své rozhodnutí a dále tím hrozí narušit fungování systémů kritické informační infrastruktury a kritické infrastruktury státu. Ani podkapitola 5.3.3 návrhu Mechanismu s ohledem na výčet okolností umožňujících prodloužení lhůty či přerušení řízení nedává jasnější představu o délce řízení. Žádáme NÚKIB o vysvětlení.
	3. Podkapitola 5.2.1 návrhu Mechanismu dále ohrožuje stabilitu systémů kritické informační infrastruktury a kritické infrastruktury tím, že zakazuje provozovatelům sítí elektronických komunikací odebírat dodávky od jiných než prověřených subjektů. Zejména za situace, kdy hrozí provozovateli nebo třetím stranám újma anebo kdy je nezbytné upravit parametry či nastavení sítí je tak v podstatě vyloučeno závadný stav odstranit a přejít třeba k jinému dodavateli s kratší dodací lhůtou. NÚKIB tak *de facto* zasahuje do rozvoje trhu a ohrožuje jeho stabilitu. Žádáme NÚKIB o vysvětlení.
	4. Podkapitola 5.2.1 návrhu Mechanismu dále odkazuje na povinnost zahájit řízení při změní okolností. K tomu viz odst. 6 výše a otázka, zda změna firmware či software v rámci pravidelných patchů, updatů či upgradů je změnou okolností, protože právě kybernetická bezpečnost na těchto systémech stojí. Tato nejasnost dále prohlubuje obavy o nedostatečnou provázanost návrhu Mechanismu s reálným světem elektronických komunikací. Žádáme NÚKIB o vysvětlení.
	5. Závěr podkapitoly 5.2.1 pak jen podtrhuje absurditu celého návrhu Mechanismu, když pro zhodnocení dodavatele vyžaduje součinnosti jiných orgánů veřejné moci již v rámci své pravomoci do identifikace a řešení hrozeb pro Českou republiku zapojených. NÚKIB se tak snižuje do role pouhého přenašeče informací získaných jinými orgány při své vlastní činnosti a vytváří zbytečnou správně právní bariéru pro podnikání. Žádáme NÚKIB o vysvětlení.
	6. Podkapitola 5.3.2 již nepokrytě vybočuje z působnosti NÚKIB, když NÚKIB zcela nepochopitelně v rámci správního řízení zamýšlí kontrolovat oblasti z pohledu kybernetické bezpečnosti zcela nepodstatné, jako je sankční režim, porušování pravidel mezinárodního obchodu, organizační struktura apod. Tyto parametry zcela vybočují z působnosti ZKB a vytváří prostor pro korupční jednání v rámci posuzování bez jasně nastavených kritérií. Žádáme NÚKIB o vysvětlení parametrů pro posuzování těchto kritérií.
	7. V téže podkapitole na závěr NÚKIB shrnuje netransparentní parametry, pro jejichž posuzování neuvádí žádná kritéria ani relevanci. Například jaké organizace jsou přátelské a jaké nepřátelské, podle jakých kritérií se případná rizika posuzují, jak je pro kybernetickou bezpečnost relevantní oblast práv duševního vlastnictví či otázka porušování závazků v oblasti mezinárodního obchodu apod. Není už vůbec zřejmé, kdo a jak bude takové informace sbírat a vyhodnocovat, aby se jednalo o informace a parametry relevantní pro zajištění bezpečnosti sítí elektronických komunikací. Žádáme NÚKIB o vysvětlení parametrů pro posuzování těchto kritérií.
	8. Navzdory tomu, že NÚKIB je orgánem zvyklým pracovat se stanovením velikosti rizik, nerozvádí v podkapitole 5.3.3 podle jakých kritérií bude řadit dodavatele do jednotlivých rizikových kategorií. Toto je relevantní zejména s ohledem na důsledky přiřazení opatření v podkapitole 5.3.4. Žádáme NÚKIB o vysvětlení parametrů pro stanovení velikosti rizik.
	9. Podkapitola 5.4.2 návrhu Mechanismu zcela absurdně vybočuje z principů právního státu, otevírá prostor pro zvůli správního orgánu a korupční prostředí. Je nepřípustné, aby zásah do podnikání spočíval na rozhodnutí, které již v zárodku není přezkoumatelné. Tento princip je zcela nepřípustný. Žádáme NÚKIB o vysvětlení.
17. **Komentáře ke kapitole 6 návrhu Mechanismu:**
	1. Kapitola 6 ignoruje realitu dodavatelsko-odběratelských vztahů, když vylučuje možnost nákupu od prostředníka, který nemusel projít posuzováním ze strany NÚKIB. Žádáme NÚKIB o vysvětlení.
18. **Komentáře ke kapitole 7 návrhu Mechanismu:**
	1. Přechodná doba pro testování stávajících dodavatelů navržená v podkapitole 7.2 návrhu Mechanismu je nedostatečná s ohledem (i) na délku investičního cyklu různých komponentů, (ii) v současnosti probíhající výstavbu sítí 5G v návaznosti na povinnosti stanovené rozvojovými kritérii vzešlými z aukce kmitočtů 5G a (iii) nemožností kombinovat v sítích technologie více dodavatelů. Žádáme NÚKIB o vysvětlení.

S pozdravem,

**Jiří Grund**

prezident

APMS (Asociace provozovatelů mobilních sítí)

+420 604 114 054

[www.apms.cz](http://www.apms.cz/)

1. Programové prohlášení vlády České republiky dostupné na internetových stránkách vlády České republiky zde: <https://www.vlada.cz/assets/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-Petra-Fialy.pdf> [↑](#footnote-ref-1)
2. <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_cs> [↑](#footnote-ref-2)
3. https://www.reuters.com/markets/asia/ericssons-isis-fallout-could-go-beyond-big-fines-2022-02-16/ [↑](#footnote-ref-3)
4. https://www.novinky.cz/internet-a-pc/clanek/nokia-zajistovala-v-rusku-spehovaci-site-fsb-40392018 [↑](#footnote-ref-4)
5. https://www.reuters.com/business/nokia-says-has-launched-legal-challenge-5g-exclusion-romania-2022-03-31/ [↑](#footnote-ref-5)
6. K dlouhodobému špiclování spojenců ze strany Spojených států amerických viz např. zde: <https://www.irozhlas.cz/zpravy-svet/odposlouchavani-zpravodajske-sluzby-cia-bnd-americane-nemci_2002112032_jgr> [↑](#footnote-ref-6)
7. K působnosti NÚKIB viz § 21a násl. ZKB. [↑](#footnote-ref-7)
8. K péči řádného hospodáře viz § 159 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, § 51 odst. 2 zákona č. 90/2012 Sb., zákon obchodních společnostech a družstvech. [↑](#footnote-ref-8)
9. K provádění důkazů ve správním řízení viz § 51 a násl. zákona č. 500/2004 Sb., správní řád, ve spojení s § 6 odst. 2 správního řádu. [↑](#footnote-ref-9)