21. 10. 2025

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

Nový zákon o kritické infrastruktuře a jeho provázanost s novým zákonem o kybernetické bezpečnosti. Kontext a přijetí nové legislativy

Dne 19. srpna 2025 nabyl účinnosti zcela nový zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (dále jen „ZoKI“). Tento zákon vyjímá problematiku kritické infrastruktury z dosavadního krizového zákona a zavádí samostatnou právní úpravu odolnosti kritických subjektů. Nová úprava reaguje zejména na požadavky směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (dále jen „CER“)[1], kterou transponuje do českého právního řádu. Cílem ZoKI je posílit odolnost základních služeb nezbytných pro fungování státu a připravit tak Českou republiku na současné hrozby, jako jsou kybernetické útoky či sabotáž kritických systémů.[2]

1. listopadu 2025 nabude účinnosti další klíčový předpis, kterým je zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**KybBez**“). Tento zákon **zcela nahrazuje dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti**, přičemž transponuje směrnici 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 (dále jen „**NIS 2**“).[3] KybBez reflektuje nové požadavky této směrnice, přičemž rozšiřuje okruh povinných subjektů, mění způsob jejich identifikace, zavádí přísnější bezpečnostní opatření i postupy hlášení incidentů a klade větší důraz na odpovědnost vrcholového vedení organizací v oblasti kybernetické bezpečnosti.

Oba nové zákony jsou na specifické úrovni propojeny a představují komplexní revizi české legislativy v **oblasti bezpečnosti klíčových infrastruktur a služeb**. V důsledku toho je v našem zájmu si přiblížit změny, které tyto zákony přináší, a zejména jejich vzájemnou provázanost.

Zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury

ZoKI uvádí do praxe požadavky směrnice CER a komplexně upravuje povinnosti státu i soukromých subjektů při zajišťování fungování tzv. **základních služeb.**[4] Co se týče základních služeb, jedná se např. o odvětví energetiky, dopravy, bankovnictví, zdravotnictví, dodávek vody, digitální infrastruktury, veřejné správy apod., tedy sektory odpovídající výčtu ze směrnice CER[5].

Klíčové pojmy a rozsah působnosti

ZoKI upouští od dřívějšího konceptu **prvků kritické infrastruktury** podle **zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů** (dále jen „**krizový zákon**“) a zavádí kategorii **subjektu kritické** infrastruktury (dále jen „**subjekt KI**“). **Poskytovatelem základní služby** je dle zákona každý, kdo poskytuje alespoň jednu základní službu na území ČR a současně splňuje stanovené kritérium významnosti[6] (hodnotící dopady narušení služby).[7] Pokud narušení poskytované služby může mít významný dopad na fungování státu či bezpečnost, pak se její poskytovatel **zařazuje mezi subjekty KI**. Subjekty KI budou nově evidovány **v seznamu subjektů KI**. O zařazení poskytovatele na seznam subjektů KI rozhoduje Ministerstvo vnitra na základě

posouzení, zda daný poskytovatel splňuje kritéria významnosti, jak bylo již výše zmíněno. Tento přístup nahrazuje původní systém určování jednotlivých prvků KI ústředními správními úřady, jelikož těžiště se posouvá na identifikaci celých subjektů, resp. organizací, které zajišťují základní služby. Změna terminologie se promítla i do souvisejících zákonů, kde například nově budou investice podléhat povolení, pokud cílí na společnost v postavení subjektu KI namísto dřívějšího pojmu provozovatele prvku KI.[8]

ZoKI vymezuje také další související pojmy. **Kritickou infrastrukturou** se rozumí aktivum, sítě, zařízení či systémy nezbytné pro poskytování základní služby.[9] ZoKI zavádí pojmy jako **kritický dodavatel**[10] či **manažer kritické infrastruktury**[11] apod.

Povinnosti subjektů KI

Nová právní úprava zavádí ucelený soubor povinností pro subjekty KI s cílem posílit **jejich odolnost vůči hrozbám různého druhu.**[12] Mezi hlavní povinnosti těchto subjektů patří zejména:

- **Poskytování informací a spolupráce s orgány veřejné moci:** Subjekt KI je povinen na základě předchozího sebeposouzení informovat kompetentní orgány o tom, jaké základní služby poskytuje, jaká kritická infrastruktura se na území ČR nachází, označit kritické dodavatele a určit manažera kritické infrastruktury apod. Dále musí oznamovat, ve kterých členských státech EU poskytuje své základní služby. Tyto informace slouží státu k efektivnímu mapování kritických souvislostí a přeshraničních vazeb.[13]
- **Analýza rizik a plánování odolnosti:** Subjekt KI je povinen **zpracovat a pravidelně aktualizovat posouzení rizik** týkající se jeho základní služby a kritické infrastruktury, a to včetně různých typů hrozeb. Na základě této analýzy musí vypracovat **plán odolnosti** s přehledem opatření k předcházení a zvládání identifikovatelných rizik. Dále má povinnost poskytovat podklady Ministerstvu vnitra pro zpracování celostátního posouzení rizik České republiky v oblasti KI.[14]
- **Opatření k zajištění odolnosti:** Subjekty KI musí přijmout a realizovat přiměřená **bezpečnostní a preventivní opatření** ke zvýšení své odolnosti.[15] Pokud subjekt KI již plní obdobné povinnosti podle jiných předpisů EU, zákon umožňuje režim rovnocennosti, kde se taková opatření uznají jako splnění povinností podle ZoKI, aby nedocházelo ke zdvojení regulace.[16]
- **Hlášení incidentů:** Významnou novinkou je povinnost hlásit **závažné incidenty ohrožující poskytování základní služby**. Subjekt KI musí nahlásit incident, který podstatně naruší nebo značí významné ohrožení kontinuity služby, kompetentnímu orgánu (zpravidla Ministerstvu vnitra) ve stanovené lhůtě. Tato povinnost koresponduje s požadavky směrnice CER na notifikaci narušení kritických činností. ZoKI zároveň stanoví, že pokud má subjekt obdobnou povinnost hlášení již podle jiného předpisu srovnatelného účinku (např. hlášení kybernetických incidentů podle KybBez), nemusí stejný incident hlásit duplicitně podle ZoKI[17]
- **Portál kritické infrastruktury:** Ministerstvo vnitra zřídí nový **informační systém**[18], jehož prostřednictvím budou subjekty KI plnit vybrané ohlašovací a informační povinnosti **elektronicky**. Použití portálu je považováno za splnění povinnosti dle ZoKI. Portál má usnadnit komunikaci a sdílení informací mezi subjekty KI a orgány veřejné moci.

ZoKI upravuje výkon státního dozoru nad plněním povinností subjektů KI a obsahuje sankční ustanovení v případě spáchání přestupku v oblasti kritické infrastruktury. Například za nesplnění povinnosti poskytnout informace, vypracovat analýzu rizik, nahlásit incident či umožnit kontrolu hrozí subjektu KI pokuta. ZoKI umožňuje udělení pokuty až do výše 50.000.000, - Kč. Zvláštní ustanovení ZoKI zavádí povinnosti Ministerstva vnitra a dalších příslušných úřadů ve vztahu k tzv. **poradním misím (advisory missions dle CER)**, které představují expertní týmy vyslané k

prověření opatření přijatých u subjektů evropské kritické infrastruktury, včetně povinnosti spolupráce těchto subjektů evropské kritické infrastruktury s poradními misemi.[19]

ZoKI rovněž novelizuje řadu souvisejících zákonů k zajištění souladu právního řádu s novou úpravou. Do zákona o svobodném přístupu k informacím bylo doplněné omezení, že informace, jejichž zveřejnění by mohlo ohrozit zajištění odolnosti a ochrany kritické infrastruktury, se neposkytují (obdobně jako je tomu u informací o kybernetické bezpečnosti). Změny se promítly i do zákona o integrovaném záchranném systému a dalších předpisů, včetně harmonizace s KybBez a s prověřováním zahraničních investic.[20].

Vzájemná propojenost ZoKI a KybBez

ZoKI a KybBez tvoří dva pilíře zabezpečení klíčových služeb státu, kterými jsou **fyzická a organizační odolnost na straně jedné a kybernetická bezpečnost na straně druhé**. Byť každý zákon transponuje odlišnou evropskou směrnici a zaměřuje se na jiný aspekt, v praxi se významně prolínají.

Především **mnohé subjekty budou podléhat oběma zákonům současně**. Typicky poskytovatelé základních služeb v energetice, finančnictví, zdravotnictví či digitální infrastruktuře budou **jednak subjekty KI** podle ZoKI, **jednak regulovanými osobami** (poskytovateli regulovaných služeb[21]) dle KybBez (pokud provozují informační sítě a systémy významné pro svou činnost, což prakticky vždy ano). Zákonodárce na tuto skutečnost pamatoval a zakomponoval do obou předpisů mechanismy pro zajištění koordinace a zamezení duplicit:

- **Automatické zahrnutí subjektů KI do působnosti KybBez:** Nové ustanovení § 5 písm. d) KybBez stanoví, že služba poskytovaná subjektem kritické infrastruktury (dle ZoKI) se považuje za regulovanou službu. Tím je zajištěno, že jakmile je určitý subjekt zařazen na seznam KI, bude de facto spadat i pod režim kybernetické bezpečnosti a plnit odpovídající povinnosti (např. zavést kybernetická opatření, hlásit kyberincidenty Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**")). NÚKIB na svých webových stránkách výslovně uvádí, že jakýkoliv subjekt spadající pod KoZI spadá do vyššího režimu povinností v rámci KybBez.[22] Praktickým dopadem je prolnutí evidence subjektů KI a registru regulovaných služeb vedeného NÚKIB. Subjekt KI **není** automaticky poskytovatelem strategicky významné služby podle KybBez.
- **Rovnocennost opatření a nesouběžná aplikace povinností:** ZoKI obsahuje ustanovení § 27 o vztahu k odvětvovým předpisům EU. Pokud má subjekt KI obdobné povinnosti již podle jiného předpisu EU nebo zákona, kterým se takový předpis provádí**, a tyto povinnosti mají srovnatelný účinek jako požadavky ZoKI**, pak se na ně povinnosti zavést odolnostní opatření a hlásit incidenty podle ZoKI **nebudou uplatňovat**. V praxi to znamená, že například banky, subjekty digitální infrastruktury či energetické společnosti, na něž dopadá KybBez nebo sektorové bezpečnostní regulace EU, nebudou nuceny opakovaně plnit totožné povinnosti.
- **Úzká spolupráce dozorových orgánů:** Dozor v oblasti KI vykonává Ministerstvo vnitra, zatímco v oblasti kybernetické bezpečnosti je dozorovým orgánem NÚKIB. Oba orgány však musí spolupracovat. Nová úprava předpokládá například koordinaci **při identifikaci subjektů KI**, v rámci níž NÚKIB bude nadále navrhovat vládě určení kritické infrastruktury v oblasti komunikačních a informačních systémů. Ústřední správní úřady (včetně NÚKIB) mají povinnost informovat Ministerstvo vnitra o každém prvku kritické infrastruktury, který určily ve své působnosti. To zaručuje, že kyberneticky významná infrastruktura je zohledněna i v režimu KI. Zároveň NÚKIB nově získá přístup k informacím z oblasti prověřování zahraničních investic týkajících se kritických a strategických dodavatelů, což umožní posoudit rizika v dodavatelském řetězci regulovaných služeb.
- **Sektorové výjimky a rozdělení působnosti:** Oba zákony reflektují, že některé sektory jsou

již regulovány jinými předpisy, a právě proto upravují své působnosti. ZoKI omezuje rozsah svých povinností pro subjekty v odvětvích **bankovnictví, finanční infrastruktury** a **digitální infrastruktury**, jelikož těmto subjektům se ukládá jen omezený výčet povinností (zejména informačních) a ostatní požadavky, např. detailní odolnostní opatření či hlášení incidentů, se primárně řídí sektorovou regulací (pro banky např. požadavky ČNB, pro digitální infrastrukturu KybBez)[23]. Naopak KybBez se nevztahuje na systémy zpracovávající utajované informace či na některé specifické vojenské a bezpečnostní složky, které mají vlastní režim.

Celkově lze říci, že ZoKI a KybBez jsou **komplementární**. Prvně jmenovaný z nich vytváří rámec **pro odolnost kritických služeb** obecně (tzv. all-hazards přístup[24], zahrnující fyzickou ochranu, personální a procesní bezpečnost, krizovou připravenost atd.), zatímco druhý se specializuje na **ochranu před kybernetickými hrozbami** a zajištění bezpečnosti informačních a komunikačních systémů. Oba zákony společně reagují na aktuální bezpečnostní výzvy a zvyšují **celkovou schopnost státu i klíčových soukromých subjektů předcházet krizovým situacím a zvládat je.**

Závěr

Nový zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti představují **největší koncepční změnu v oblasti národní bezpečnosti od roku 2014 (kdy nabyl účinnosti stávající zákon č. 181/2014 Sb., o kybernetické bezpečnosti)**. ZoKI reaguje na potřebu komplexní ochrany základních služeb státu před všemi typy hrozeb, zatímco KybBez implementuje aktuální požadavky na digitální bezpečnost v souladu s evropskými standardy NIS 2. Oba předpisy přinášejí nové povinnosti pro široký okruh subjektů od provozovatelů infrastrukturních sítí, přes nemocnice a finanční instituce, až po digitální služby a veřejnou správu. Současně však vytvářejí propojený systém, který se vyhýbá duplicitám a naopak podporuje vzájemnou spolupráci.

Z pohledu kontinuity právní úpravy je podstatné, že KybBez **nahrazuje dosavadní zákon** č. 181/2014 Sb., o kybernetické bezpečnosti a od 1. listopadu 2025 převezme veškerou jeho agendu. Stejně tak agenda kritické infrastruktury **byla vyčleněna z krizového zákona** a od 19. srpna 2025 ji upravuje ZoKI. Hlavní změny oproti předchozím úpravám zahrnují **rozšíření okruhu regulovaných subjektů**, **zavedení nových kategorií služeb a povinností**, posílení role **orgánů dohledu** a celkové zpřísnění požadavků na bezpečnost a odolnost. Pro subjekty spadající do působnosti těchto zákonů bude následující období znamenat nutnost se s novými pravidly důkladně seznámit a **adaptovat interní procesy**.

Z legislativního hlediska představují oba zákony **propojený celek**, který by měl zajistit, že **kritické služby v České republice budou řádně chráněny před fyzickými i kybernetickými hrozbami**. Český právní řád se tak posouvá k modernímu systému ochrany kritické infrastruktury a kyberprostoru, jenž odpovídá aktuálním evropským trendům i bezpečnostní situaci. Jedná se o významný krok ke zvýšení bezpečnosti státu i jeho občanů v nadcházejících letech.

Samuel Kovalčík

Weinhold Legal

Weinhold Legal, s.r.o. advokátní kancelář

Florentinum
Na Florenci 15
110 00 Praha 1

Tel.: +420 225 385 333
Fax: +420 225 385 444
e-mail: wl@weinholdlegal.com

---

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES. Úřední věstník EU, L 333, 27. 12. 2022, s. 164–196. Dostupné >>>zde.

[2] K dispozici >>> zde.

[3] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké úrovně kybernetické bezpečnosti v Unii. Úřední věstník EU, L 333, 27. 12. 2022, s. 80–152. Dostupné >>> zde.

[4] Základní službou se rozumí taková služba, která je nezbytná pro zachování základních funkcí státu, ekonomiky, bezpečnosti, veřejného zdraví či životního prostředí, a která je poskytována v některém z vymezených odvětví nebo pododvětví uvedených v příloze zákona

[5] K dispozici >>> zde.

[6] určuje význam narušení poskytování základní služby na základě jednotlivých ukazatelů jmenovaných v § 10 odst. 1 ZoKI

[7] § 2 odst. 1 písm. b) ZoKI

[8] K dispozici >>> zde.

[9] § 2 odst. 1 písm. c) ZoKI

[10] dodavatel zboží či služeb nezbytných pro zajištění základní služby

[11] má na starosti koordinaci plnění povinnosti, komunikaci s úřady a implementaci bezpečnostních opatření

[12] např. přírodní katastrofy, technické havárie, terorismus i kybernetické útoky

[13] § 14 odst. 1 písm. a), g) a j) ZoKI

[14] § 14 odst. 1 písm. d), e) a f) ZoKI

[15] např. fyzická ochrana infrastruktury, záložní zdroje, bezpečnostní postupy, ochrana proti kybernetickým hrozbám apod.

[16] § 26 odst. 1 ZoKI

[17] § 27 odst. 1 ZoKI

[18] Portál kritické infrastruktury – povinnost podle § 6 odst. 1 písm. e) ZoKI

[19] § 26 ZoKI

[20] K dispozici >>> zde.

[21] jde o službu, o níž Národní úřad pro kybernetickou a informační bezpečnost rozhodne, že splňuje stanovené podmínky významnosti podle § 4 KybBez

[22] https://portal.nukib.gov.cz/informacni-servis/faq/faq-novy-zakon-o-kyberneticke-bezpecnosti

[23] § 28 ZoKI

[24] pojem vychází přímo ze směrnice CER a prakticky to znamená, že subjekty kritické infrastruktury musí při posuzování rizik zohlednit všechny relevantní typy hrozeb, nikoli pouze jeden vybraný typ

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu

- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory