

Český telekomunikační úřad (dále jen „Úřad“) jako příslušný orgán státní správy podle § 108 odst. 1 písm. b) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „zákon“), a zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, na základě výsledků veřejné konzultace uskutečněné podle § 130 zákona, rozhodnutí Rady Úřadu podle § 107 odst. 9 písm. b) bod 2 a k provedení § 15 odst. 8 zákona vydává

**opatření obecné povahy č. OOP/X/xx.2022-y,  
kterým se stanoví rozsah údajů o individuálních oprávněních k využívání rádiových  
kmitočtů vyloučených ze zpřístupnění.**

**Článek 1  
Úvodní ustanovení**

Toto opatření obecné povahy stanoví rozsah údajů o individuálních oprávněních k využívání rádiových kmitočtů (dále jen „oprávnění“), které jsou vyloučeny ze zpřístupnění.

**Článek 2  
Rozsah údajů vyloučených ze zpřístupnění**

(1) Údaje podle § 15 odst. 7 zákona o oprávnění pevné služby se vylučují ze zpřístupnění v plném rozsahu.

(2) Údaje podle § 15 odst. 7 zákona o oprávnění pohyblivé služby se vylučují ze zpřístupnění v plném rozsahu.

(3) Údaje o oprávnění vyloučené v odstavci 1 a 2 lze zpřístupnit výhradně v případě, požádá-li o zpřístupnění držitel příslušného oprávnění.

**Článek 3  
Účinnost**

Toto opatření obecné povahy nabývá účinnosti dnem 1. července 2022.

**Odůvodnění**

Úřad vydává k provedení § 15 odst. 8 zákona opatření obecné povahy č. OOP/X/xx.2022-y, kterým se stanovují údaje o individuálních oprávněních k využívání rádiových kmitočtů (dále jen „oprávnění“), které jsou vyloučeny ze zpřístupnění.

Podle § 15 odst. 6 zákona Úřad pro účely výkonu správy rádiového spektra a kontroly elektronických komunikací, vyhledávání a odstraňování zdrojů rušení rádiových kmitočtů a pro kontrolu a vyhodnocení plnění podmínek, které byly uloženy držiteli přidělu rádiových kmitočtů podle § 22 ve výběrovém řízení podle § 21, vede databázi přidělených rádiových kmitočtů s informacemi zejména o číslech rozhodnutí, kterými byly rádiové kmitočty přiděleny, a době, na kterou byly přiděleny. Databáze je veřejně přístupná způsobem umožňujícím dálkový přístup.

Veřejný přístup není k údajům o osobě držitele oprávnění podle § 18 zákona, pokud je držitel fyzickou osobou, a o rádiových kmitočtech přidělených

- a) Ministerstvu vnitra pro účely bezpečnosti státu,
- b) Policii České republiky pro účely bezpečnosti státu,
- c) Bezpečnostní informační službě,
- d) Vězeňské službě České republiky,
- e) Hasičskému záchrannému sboru České republiky,
- f) Ministerstvu obrany pro vojenské účely,
- g) Celní správě České republiky,
- h) Generální inspekci bezpečnostních sborů,
- i) Úřadu pro zahraniční styky a informace.

Podle § 15 odst. 7 zákona Úřad k části databáze vedené podle § 15 odst. 6 zřizuje a provozuje informační portál (dále též „portál“), jehož prostřednictvím zpřístupní informace o využívání rádiových kmitočtů v **pevné, pohyblivé a rozhlasové** radiokomunikační službě v sítích elektronických komunikací v rozsahu těchto údajů:

- a) osoba držitele oprávnění podle § 18,
- b) název a geografické souřadnice stanoviště rádiových stanic,
- c) nadmořská výška stanoviště rádiových stanic,
- d) vyzářený výkon rádiové stanice nebo výkon přivedený do antény,
- e) přidělený rádiový kmitočet nebo kanál a jeho šířka.

Je-li to nezbytné pro zajištění správy a účelného využívání rádiového spektra může Úřad podle § 15 odst. 8 zákona opatřením obecné povahy vyloučit ze zpřístupnění některé údaje podle § 15 odst. 7 zákona. Úřad může tyto údaje rovněž vyloučit ze zpřístupnění na základě podnětu držitele oprávnění, a to z důvodu zajištění bezpečnosti sítí elektronických komunikací nebo informací podle jiných právních předpisů (zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti).

Pro úplnost je třeba uvést, že přístup veřejnosti k údajům v portálu, jejichž zpřístupnění nebylo vyloučeno opatřením obecné povahy podle § 15 odst. 8 zákona, má být umožněn bezplatně po ověření totožnosti tazatele. Úřad je k tomu účelu oprávněn zpracovávat osobní údaje osob, kterým byly prostřednictvím portálu zpřístupněny údaje podle § 15 odst. 7 zákona, a v nezbytném rozsahu předávat tyto údaje držitelům oprávnění.

Jak z předmětné právní úpravy vyplývá, je dán obecný zájem na přístupnosti některých zákonem definovaných informací o oprávnění a v určité specifické části (oprávnění pro využívání rádiových kmitočtů v pevné, pohyblivé a rozhlasové radiokomunikační službě) i k některým detailnějším údajům o obsahových náležitostech těchto oprávnění (§ 15 odst. 7 zákona). Výjimky z rozsahu informací ke zpřístupnění jsou dány jak samotným zákonem (§ 15 odst. 6 zákona), tak je možno rozsah údajů podle § 15 odst. 7 zákona omezit Úřadem, jsou-li pro takové omezení dány zákonem stanovené podmínky, a to ve formě opatření obecné povahy z moci úřední Úřadu, nebo na základě podnětu držitele oprávnění.

K tomu Úřad uvádí, že dne 28. února 2022 obdržel podnět jednoho z držitelů oprávnění, s odvoláním na potřebu zajištění bezpečnosti jeho sítě elektronických komunikací a informací podle jiných právních předpisů a požaduje ze zpřístupnění podle § 15 odst. 7 zákona vyloučit zejména údaje v tomto ustanovení pod písmeny b) až e). Podavatel podnětu zdůrazňuje, že je správcem a provozovatelem kritické infrastruktury, správcem a provozovatelem kritické informační infrastruktury a současně je osobou s přístupem k utajovaným informacím podle zákona č. 412/2005 Sb., to vše ve vazbě na rádiové kmitočty využívané na základě oprávnění, na která dopadá obecný požadavek na zpřístupnění údajů na portálu.

V návaznosti na tento podnět, a protože důvody uváděné podavatelem podnětu jsou nepochybně platné i pro další dotčené držitele oprávnění, zahájil Úřad posouzení, zda a v jakém rozsahu je nezbytné některé údaje ze zpřístupnění vyloučit a zda stejná míra ochrany údajů

přísluší i dalším údajům (jiných držitelů oprávnění), které by bylo ze zpřístupnění rovněž nutné vyloučit.

Pro volbu konkrétního výčtu údajů vyloučených ze zpřístupnění je účelné nejprve vyhodnotit kritéria nezpřístupnění. Úřad v rámci posuzování možnosti a rozsahu vyloučení údajů ze zpřístupnění dospěl k následujícím zjištěním:

1. Zpřístupnění dodatečných údajů o oprávnění nad rámec údajů zpřístupňovaných v současné době způsobí, že jsou tyto údaje již navždy znehodnoceny z hlediska jejich ochrany v případě, že by se tyto údaje v čase staly citlivými z pohledu bezpečnosti sítí elektronických komunikací nebo informací (a to včetně kybernetické bezpečnosti). Pokud by v čase došlo k označení těchto údajů (respektive oprávnění) jako citlivých, tj. nevhodných ke zpřístupnění, tím, že byly v minulosti zpřístupněny a od určitého okamžiku by již zpřístupněny nebyly, jedná se fakticky o přímé oznámení údajů, které jsou citlivé (a zpřístupněné). To, zda konkrétní oprávnění je nadále platné je možné snadno ověřit z webových stránek Úřadu, neboť Úřad je povinen podle § 15 odst. 6 zákona vést a dálkově zpřístupnit databázi přidělených rádiových kmitočtů s informacemi o číslu rozhodnutí (oprávnění) a dobu přidělení. Tento rozsah informací (zpřístupněn již v současné době) platí jednak pro všechna oprávnění, tedy nikoliv jen pro oprávnění pro pevnou, pohyblivou nebo rozhlasovou službu, a rovněž se na něj nevztahuje možnost vyloučení některých těchto údajů ze zpřístupnění podle § 15 odst. 8 zákona.
2. Úřad dále vzal v potaz oblast provozovatelů kritické infrastruktury, respektive samu kritickou infrastrukturu anebo správce a provozovatele kritické informační infrastruktury podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“). Kritická infrastruktura je infrastruktura, která je klíčová pro chod společnosti a ekonomiky. Její ochrana je nanejvýše důležitá, zejména pro případy krizových situací. Krizová situace pak může zásadně ovlivnit či ohrozit život či bezpečnost obyvatelstva, nebo způsobit škody na majetku. Z tohoto důvodu je zcela nezbytné, aby informace související s využíváním rádiových kmitočtů a kritickou infrastrukturou, zejména pak údaj o osobě držitele oprávnění a souřadnice stanoviště vč. nadmořské výšky, nebyly zpřístupněny. Jejich zpřístupnění zvyšuje riziko úmyslného ohrožení, a to jak už fyzického (zničení např. napájení telekomunikační techniky, porušení statiky budovy/stožáru apod.), tak i záměrné způsobování škodlivého rušení, které znemožní samotnou komunikaci. Dotčení držitelé oprávnění využívají rádiové kmitočty jak pohyblivé, tak i pevné služby.
3. Úřad dále identifikoval řadu dalších sektorových oblastí, které jsou zcela nezbytné pro plynulý chod společnosti a ekonomiky, a jejichž ohrožení by vedlo k nepřiměřenému riziku vzniku škod na majetku a ohrožení životů nebo bezpečnosti občanů (ať už např. prostřednictvím teroristického činu či nehody) a to i za situace, kdy se nejedná o kritickou infrastrukturu. Typicky se může jednat o důlní společnosti, které využívají rádiové kmitočty nejen za účelem ochrany objektu, ale také při dispečerské a jiné komunikaci související se získáváním a distribucí základní komodity, jako je např. uhlí. Obdobně lze dále identifikovat oblasti energetiky, teplárenství, plynárenství, dopravy, zdravotnictví (nemocnice), vodárenství apod. I v tomto případě, zpřístupnění dodatečných informací nad rámec těch, které jsou zpřístupněny před 1. červencem 2022, může vést ke zcela zbytečnému ohrožení obyvatelstva a majetku či zásobování důležitými komoditami. Dotčení držitelé oprávnění využívají rádiové kmitočty jak v rámci pohyblivé, tak i pevné služby.
4. Existují však dále držitelé oprávnění, kteří sice neposkytují, či nedistribuuji zásadní komodity, jako je např. uhlí, ropa, voda, elektřina, teplo, plyn atd., ale jsou odpovědní za včasné a rychlé informování obyvatelstva v případě živelné katastrofy a krizové situace. Mezi tyto subjekty se řadí řada obcí či na ně navázané subjekty, jako je např. městská policie, technické služby měst či obcí apod. Odhalení lokality umístění dotčených vysílacích rádiových zařízení nepřiměřeně

zvyšuje riziko jejich poškození, sabotáže, a to zejména v době krize či vyšší bezpečnostní hrozby.

5. Úřad dále identifikoval řadu dalších provozovatelů, kteří jsou poskytovateli služeb elektronických komunikací a mezi jejichž zákazníky patří orgány veřejné moci a organizační složky státu. Orgány veřejné moci a organizační složky státu jsou také jako správci tzv. významných informačních systémů ve velké míře zastoupeni v rámci regulace ZokB, což jen podtrhuje význam jejich ochrany. Jakékoliv ohrožení možnosti využívání rádiových kmitočtů těmito subjekty je tak i v tomto případě nežádoucí, zejména v době krize či vyšší bezpečnostní hrozby. Tito držitelé využívají rádiové kmitočty jak v rámci pevné, tak i pohyblivé služby.
6. Úřad si je vědom dalších skupin držitelů oprávnění, kteří zajišťují i jiné služby, než je uvedeno výše. Primárně nejsou tyto služby podstatné z hlediska vzniku případné krizové situace či ohrožení majetku či ohrožení bezpečnosti a života občanů. Typicky se jedná o držitele oprávnění využívající rádiové kmitočty např. pro účely podnikání v turistice, poskytování nadstandardních dopravních služeb, využívání rádiových kmitočtů pro zájmové činnosti a další. Nicméně, tyto držitelé oprávnění často využívají pro šíření jim přidělených rádiových kmitočtů taková stanoviště, která jsou často využívána i držiteli oprávnění, jejichž využívání je potřeba informačně chránit. Pokud by tak Úřad zpřístupnil i tuto množinu oprávnění včetně dodatečných informací (zejména pak souřadnice stanoviště vč. nadmořské výšky), mohl by tím Úřad nepřímo napomoci odhalit významné telekomunikační body sítě. Taková situace je však nežádoucí. Bezpečnost (zejména ta fyzická) je velmi důležitá, neboť tyto telekomunikační body zpravidla agregují i další provoz důležitých subjektů z hlediska bezpečnosti sítí elektronických komunikací nebo informací. Vedlejším efektem zpřístupnění oprávnění této, na první pohled mylně nedůležité, množiny držitelů tak Úřad nechtěně může napovědět, jaké lokality jsou z hlediska rádiové infrastruktury důležité a kritické.
7. Úřad současně identifikoval, že některé informace o některých oprávněních je nutno chránit i z dalších důvodů. Typickým příkladem jsou krátkodobá oprávnění, která Úřad uděluje na základě žádosti Ministerstva zahraničních věcí pro zajištění bezpečnosti důležitých zahraničních návštěv, nebo oprávnění udělovaná pořadatelům hromadných sportovních nebo společenských akcí. I v těchto případech jakékoliv ohrožení nebo narušení komunikačních systémů může vést k ohrožení nebo snížení bezpečnosti chráněných osob, nebo v případě akcí s velkým počtem účastníků může ztížit nebo znemožnit jakékoliv řešení případně vzniklých krizových situací nebo stavů.
8. Úřad v rámci úřední činnosti také zjistil, že někteří držitelé oprávnění mají přístup k utajovaným informacím ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací (dále jen „UI“) a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Vyzrazení nebo zneužití UI může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné. Přestože jsou UI zpravidla zpracovávány v izolovaných systémech, v návaznosti na bod č. 6 tohoto odůvodnění, vyzrazení (či jen odhadnutí) souřadnic významných bodů telekomunikační infrastruktury může vést k ohrožení přenosu těchto informací a vyvolat nepříznivé důsledky spojené s přerušením toku takových informací.
9. Úřad dospěl také ke zjištění, že i v rámci jednoho držitele oprávnění by bylo nutné, aby Úřad přistoupil k vyloučení všech oprávnění tohoto držitele oprávnění. Úřad totiž oprávněně předpokládá, že může být pro držitele oprávnění prakticky nerealizovatelné a velmi administrativně a finančně náročné odlišit ty části telekomunikační sítě, které jsou sdílené pro „nekrizové“ a „krizové“ řízení. Současně, každou konfiguraci sítě by bezesporu muselo být provedeno posouzení z hlediska poměru sdílení sítě, což je rovněž pro dotčeného držitele oprávnění velká administrativní, ale i finanční zátěž. V neposlední řadě by taková činnost zatížila i nepřiměřeným způsobem samotný Úřad. Dále, nepochybně by okamžik rozhodnutí Úřadu o nezpřístupnění nové množiny oprávnění dotčeného držitele mělo určité časové zpoždění a nedokázalo by promptně reagovat na případné změny ve využívání rádiových kmitočtů, respektive konfiguraci sítě. To by v konečném důsledku znamenalo zpřístupnění informace, která by již z pohledu držitele oprávnění neměla být vůbec zpřístupněna. Navíc, jak bylo naznačeno

výše, samotným aktem nezpřístupnění již v minulosti zpřístupněné informace může být odhadnuto, že taková informace je hlubšího významu a je určitým způsobem pro držitele oprávnění citlivá, když se rozhodl ji Úřad nově nezpřístupnit. Z tohoto důvodu nedává Úřadu jiný smysl než v obecné rovině uvažovat celou množinu oprávnění, jejichž je dotčený subjekt držitelem. Pro dokreslení celé situace, systémy kritické infrastruktury, významné informační systémy, provozovatelé základní služby a další jsou podle ZoKB určovány průběžně a bez přičinění Úřadu. V takových případech se Úřad dozví opět se zpožděním o důležitosti informace. Co se týče ostatních subjektů (primárně body č. 3, č. 5 a č. 6 tohoto odůvodnění), Úřad by musel kontinuálně prověřovat všechny subjekty, respektive držitele oprávnění. I v těchto případech by znepřístupnění informací bylo s časovým zpožděním. Za další negativní efekt pak lze považovat již výše zmíněnou administrativní náročnost celého procesu. Tato množina znepřístupněných informací by musela být zkoumána nejen z hlediska nově přibývajících informací, ale také z hlediska redukce těch informací, které lze již zpřístupnit.

10. Úřad vnímá, že důležitost sítí elektronických komunikací a služeb na nich poskytovaných v čase neustále roste tak, jak postupuje digitalizace státu i života občanů. Tato situace ale bezesporu s sebou přináší i nutnost zajištění robustní bezpečnosti, integrity a odolnosti těchto sítí a služeb nejen proti případným technickým výpadkům, ale i proti případným útokům ze strany nejrůznějších subjektů. Za toto zajištění jsou primárně zodpovědní držitelé oprávnění. Nicméně, Úřad by měl postupovat tak, aby tuto snahu držitelů oprávnění nedegradoval, neznehodnocoval a aby zbytečně nezavdával větší možnosti (úspěšným) pokusům o kybernetické, ale i fyzické útoky na telekomunikační sítě a služby elektronických komunikací, dále snahy o získání citlivých informací či zneužití informací jak pro narušení výše uvedených služeb kriticky důležitých pro zajištění bezpečnosti služeb a fungování státu.
11. V neposlední řadě lze dojít k důležitým informacím „vylučovací metodou“. Pokud by například došlo v terénu k faktické identifikaci využívání rádiových kmitočtů, a takové využívání, respektive údaje uvedené v oprávnění v rozsahu § 15 odst. 7 zákona, by nebyly dohledány v informačním portálu vedeném podle daného ustanovení Úřadem, bylo by možné snadno dovodit, že se pravděpodobně jedná o takové využívání rádiových kmitočtů, jehož parametry (údaje uvedené v oprávnění) byly veřejnosti znepřístupněny z důvodu zajištění bezpečnosti sítí elektronických komunikací nebo informací. Takto by fakticky došlo ke zpřístupnění údajů, které s ohledem na právem chráněné zájmy nemají být zpřístupněny.

Rusko-ukrajinský konflikt probíhající v současné době na území Ukrajiny, může ve svém důsledku představovat bezpečnostní hrozbu, resp. výrazně zvyšuje její riziko, i pro Českou republiku, respektive pro systémy kritické informační infrastruktury a další pro stát strategicky významné infrastruktury. Proto je v návaznosti na body odůvodnění uvedené výše podle Úřadu rovněž důvodné, aby detailní informace o oprávnění, využitelné kterýmkoliv nepřátelským subjektem, nebyly veřejně dostupné. Bude-li mít Úřad za to, že výše uvedené důvody pro omezení zpřístupnění údajů oprávnění pominuly, může změnou tohoto opatření obecné povahy množinu zpřístupněných údajů rozšířit.

Na základě všech výše uvedených zjištěných skutečností (body č. 1 až č. 11) a také optikou momentální bezpečnostní situace ve východní Evropě zapříčiněné ozbrojeným konfliktem na území Ukrajiny, kdy se zcela zásadně ukazuje potřeba robustních, proti kybernetickým útokům odolných komunikačních sítí a bezpečnosti infrastruktury, provedl Úřad poměření relevantních právem chráněných zájmů, v daném případě poměření mezi zájmem uživatelů rádiového spektra na dostupnosti relevantních informací o něm a veřejným zájmem na zajištění bezpečnosti sítí elektronických komunikací nebo právem chráněných informací, resp. zájmem na zajištění kybernetické bezpečnosti.

Z hlediska zájmu uživatelů rádiového spektra na dostupnosti relevantních informací je možné vycházet z důvodové zprávy k novelizaci § 15 zákona provedené zákonem č. 374/2021 Sb. Tento zájem spočívající v „právu na další informace o rádiovém spektru“ je však samotnou

novelou zákona, konkrétně ustanovením § 15 odst. 8 zákona, ve znění zákona č. 374/2021 Sb. „regulován“, a to potřebou zajištění správy a účelného využívání rádiového spektra a dále zájmem na zajištění bezpečnosti sítí elektronických komunikací nebo právem chráněných informací, je-li Úřadem tato potřeba identifikována.

S ohledem na Úřadem výše identifikovaná bezpečnostní a další rizika spojená se zpřístupněním údajů nad rozsah stávajícího rozsahu údajů dospěl Úřad k závěru, že je potřeba upřednostnit zájem na zajištění bezpečnosti sítí elektronických komunikací nebo právem chráněných informací, resp. zájmem na zajištění kybernetické bezpečnosti, před zájmem na zpřístupnění dalších informací o rádiovém spektru.

Úřad upřednostnil zájem na zajištění bezpečnosti sítí a právem chráněných informací, jejíž ohrožení může v důsledku znamenat ohrožení bezpečnosti státu a životů a zdraví osob. Jakékoli ohrožení v této kategorii zcela zásadním způsobem převažuje nad možnými negativními dopady menšího okruhu zpřístupněných informací o rádiovém spektru, resp. jejich nižší dostupnosti pro veřejnost.

Na základě Úřadem provedeného poměření právem chráněných zájmů a identifikovaná rizika spojená se zpřístupněním údajů a s vědomím toho, že jednou zpřístupněné údaje již nelze dodatečně chránit (viz bod 1 tohoto odůvodnění), se Úřad rozhodl vyloučit ze zpřístupnění celou množinu údajů podle § 15 odst. 7 zákona ve vztahu ke všem oprávněním v pevné a pohyblivé službě, když zpřístupnění dodatečných údajů nad rámec dnes dostupných Úřad považuje za nadměrně vysoké riziko z hlediska bezpečnosti sítí elektronických komunikací.

Na uvedeném závěru nemůže nic změnit ani skutečnost, že přístup veřejnosti k předmětným údajům v portálu má být umožněn až po ověření totožnosti tazatele a že Úřad je k tomu účelu oprávněn zpracovávat osobní údaje osob, kterým byly prostřednictvím portálu zpřístupněny údaje podle § 15 odst. 7 zákona, a v nezbytném rozsahu předávat tyto údaje držitelům oprávnění. Jak lze z právní úpravy jednotlivých dotčených zákonů (zákon o kybernetické bezpečnosti, krizový zákon a zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti) zřejmé, objekty jejich ochrany, tomto kontextu sítí elektronických komunikací a informace je třeba chránit a nelze jejich bezpečnost ani ohrozit. K tomu srov. § 10a zákona o kybernetické bezpečnosti, podle kterého informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti se podle předpisů upravujících svobodný přístup k informacím neposkytují. Viz také [https://nukib.cz/download/publikace/podpurne\\_materialy/Doporuceni\\_Poskytovani\\_informaci\\_v2.0.pdf](https://nukib.cz/download/publikace/podpurne_materialy/Doporuceni_Poskytovani_informaci_v2.0.pdf). Na základě výše uvedené argumentace naplňují jednotlivé informace o využití rádiového spektra daným subjektem v kontextu znaky informace, která je z hlediska zachování kybernetické bezpečnosti natolik důvěrná, že by jejím vyžrazením mohlo dojít k narušení kybernetické bezpečnosti.

Předmětné ustanovení bylo do ZoKB doplněno v rámci novely provedené zákonem č. 205/2017 Sb. (účinnost od 1. 8. 2017). Již tehdy Důvodová zpráva k tomuto zákonu jasně konstatovala, že „v současné době, kdy již bylo určeno 155 významných informačních systémů, spravovaných 58 subjekty, a 48 systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy potenciálních povinných subjektů podle zákona o svobodném přístupu k informacím, a kdy roste počet útoků v kybernetickém prostoru, je zapotřebí přistoupit k opatření i v obecnější rovině zajišťování kybernetické bezpečnosti.“. Rovněž bylo touto zprávou identifikováno, že informace, které není v zájmu zajišťování kybernetické bezpečnosti možné poskytovat, mohou být mimo jiné i například schémata, plány budov, technické specifikace (např. topologie sítě), konfigurační parametry. Tyto informace korespondují zejména s údaji podle § 15 odst. 7 písm. b) až e) zákona. Je-li jejich poskytnutí vyloučeno výjimkou ze zákona o svobodném přístupu k informacím, nelze toto bezpečnostní opatření devalvovat zpřístupněním informací podle § 15 odst. 7 zákona.

Výše uvedená zjištění o potřebě důsledné ochrany předmětných údajů jsou natolik závažná, že tím, že by dané údaje byly poskytnuty, byť tazateli s jasnou identifikací, kterou by bylo možno využít v případě, že by k narušení této vyžadované míry bezpečnosti v důsledku

zpřístupnění údajů došlo, vedou k závěru o potřebě vyloučení těchto údajů ze zpřístupnění. Zde je třeba odkázat na výše uvedené zjištění (viz bod č. 1 tohoto odůvodnění), že jednou zpřístupněné údaje jsou již navždy znehodnoceny z hlediska jejich ochrany v případě, že by se tyto údaje v čase staly citlivými z pohledu bezpečnosti sítí elektronických komunikací nebo informací (a to včetně kybernetické bezpečnosti).

V době, kdy bylo ustanovení § 15 odst. 7, 8 a 9 do zákona doplněno (provedeno zákonem č. 374/2021 Sb. s účinností od 1. ledna 2022, resp. pro případ portálu do 1. července 2022) nebylo, resp. nemohlo být se současnou mezinárodní situací počítáno. Informace podle § 15 odst. 7 zákona tak mohou být za současné situace vysoce citlivé a jejich zpřístupnění veřejnosti by mohlo mít dalekosáhlé bezpečnostní dopady.

Dále je třeba uvést, že oprávnění určuje pouze technické podmínky využívání rádiových kmitočtů. Jaké služby nebo pro jaký účel budou využity určuje vždy držitel oprávnění podle svého vlastního uvážení. Toto se také v čase může měnit, aniž by bylo třeba měnit podmínky v oprávnění. Aby tedy nebyl ohrožen žádný z výše uvedených chráněných zájmů, je třeba omezit zpřístupnění údajů v maximálním možném rozsahu, tj. v celém rozsahu § 15 odst. 7 písm. a) až e) zákona. Ve vazbě k rozsahu nezpřístupněných údajů Úřad také dospěl k závěru, že pokud by zpřístupnil např. pouze hodnotu výkonu přivedeného do antény (§ 15 odst. 7 písm. d) zákona), tak tato informace sama o sobě není citlivá, ale citlivou se stane až ve vazbě na zpřístupněné další údaje oprávnění. Nicméně, vzhledem k tomu, že samotné zpřístupnění tohoto údaje nijak nepřispěje k cíli popsaném ve výše zmíněné důvodové zprávě, a dále, že se rozsah údajů týká vždy konkrétního jednoho oprávnění, dává Úřadu smysl, takový údaj rovněž nezpřístupňovat. Současně tímto přístupem Úřad ochrání i osobu držitele oprávnění.

Nicméně, současně je potřeba deklarovat, že úmyslem Úřadu není zcela vyloučit možnost zpřístupnění, resp. zpřístupnění dalších údajů. Toto zpřístupnění však ponechává na vůli a potřebě samotného držitele oprávnění (čl. 2 odst. 3), kterému poskytuje možnost obrátit se kdykoliv na Úřad s požadavkem na zpřístupnění dodatečných informací, resp. údajů obsažených v jím držených oprávněních, pokud by potřeba této ochrany na jeho straně byla z podstaty trvalé volby držitele oprávnění irelevantní, nebo by s konečnou platností odpadla. Touto cestou je tak umožněno naplňovat i cíl předmětných ustanovení § 15 zákona, ve znění zákona č. 374/2021 Sb., směřující ke zvýšení dostupnosti a rozsahu informací o rádiovém spektru, avšak při zachování maximální a potřebné ochrany ostatních chráněných zájmů.

Nad rámec výše uvedeného Úřad dále konstatuje, že údaje o oprávnění rozhlasové služby nejsou ze zpřístupnění vyloučeny. Tyto údaje jsou již nyní volně dostupné v návaznosti na § 125 odst. 5 zákona, kdy Úřad je mj. povinen uveřejňovat informace týkající se sítí pro rozhlasovou službu podle zákona o provozování rozhlasového a televizního vysílání. V návaznosti na tuto skutečnost tak Úřad nebude přístup k těmto informacím podmiňovat ani ověřením totožnosti tazatele, jak obecně předpokládá § 15 odst. 9 zákona.

V tomto okamžiku a za daných okolností se proto Úřad rozhodl přistoupit u pevné a pohyblivé služby k omezení zpřístupnění údajů podle § 15 odst. 7 zákona.

Článek 1 stanoví předmět tohoto opatření obecné povahy, kterým je rozsah údajů o využívání rádiových kmitočtů obsažených v oprávněních, které jsou vyloučeny ze zpřístupnění.

Článek 2 stanoví v návaznosti na výše uvedené, které údaje jsou vyloučeny ze zpřístupnění a současně je v odstavci 3 tohoto článku stanovena možnost Úřadu zpřístupnit tímto opatřením obecné povahy vyloučené údaje obsažené v oprávnění v případě, že o to držitel takového oprávnění požádá.

Článek 3 stanoví účinnost opatření obecné povahy č. OOP/X/xx.2022-y, kterým se stanoví rozsah údajů o individuálních oprávněních k využívání rádiových kmitočtů vyloučených ze zpřístupnění. Účinnost byla stanovena v návaznosti na účinnost § 15 odst. 7 a násl. zákona, jejichž účinnost byla stanovena rovněž ke dni 1. července 2022 v souladu s čl. XVII zákona č. 374/2001 Sb. ze dne 15. září 2021.

\*\*\*

Na základě § 130 zákona a podle Pravidel Českého telekomunikačního úřadu pro vedení konzultací na diskusním místě Úřad zveřejnil dne **XX** návrh opatření obecné povahy č. OOP/X/xx.2022-y, kterým se stanovují údaje o individuálních oprávněních k využívání rádiových kmitočtů, které jsou vyloučeny ze zveřejnění, a výzvu k podávání připomínek na diskusním místě.

Sohledem na dopady daného opatření do oblasti kybernetické bezpečnosti a bezpečnosti státu jako takové, byl návrh opatření obecné povahy podle § 112a zákona konzultován Národním úřadem pro kybernetickou bezpečnost a v rámci obecné spolupráce i se zpravodajskými službami.

V rámci veřejné konzultace Úřad během lhůty 30 dní obdržel ...

za Radu Českého telekomunikačního úřadu:

Mgr. Ing. Hana Továrková  
předsedkyně Rady  
Českého telekomunikačního úřadu