# Důvodová zpráva

## Návrh nařízení vlády o nepominutelných funkcích stanoveného rozsahu

## I. Obecná část

### 1. Popis obsahu návrhu právního předpisu s uvedením důvodů, které k jeho předložení vedou, a shrnutí základních zásad a nejdůležitějších změn, které oproti stávající právní úpravě zavádí

V návrhu zákona o kybernetické bezpečnosti (dále jen „zákon“) zahrnujícím mechanismus prověřování bezpečnosti dodavatelského řetězce (dále jen „mechanismus posuzování dodavatelů“), dochází v § 27 odst. 2 písm. a) k zavedení pojmu „kritická část stanoveného rozsahu“. Tímto pojmem se pro potřeby mechanismu posuzování dodavatelů rozumí aktiva stanoveného rozsahu zajišťující nepominutelné funkce nebo aktiva stanoveného rozsahu, u kterých byl poskytovatelem regulované služby v režimu vyšších povinností, na kterého dopadají povinnosti z mechanismu posuzování dodavatelů, ohodnocen dopad narušení bezpečnosti informací na stanovený rozsah úrovní kritická (dále jen „kritická aktiva“).

Zákon stanovuje dva způsoby určení kritické části stanoveného rozsahu, přičemž tyto lze rozdělit na subjektivní (závislé na vůli poskytovatele regulované služby) a objektivní (nezávislé na vůli poskytovatele regulované služby).

Prostřednictvím samoidentifikace může poskytovatel regulované služby v režimu vyšších povinností u aktiv stanoveného rozsahu, postupem podle návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, ohodnotit dopad narušení bezpečnosti informací na stanovený rozsah úrovní kritická nebo vysoká. Tím se stanou kritickou součástí stanoveného rozsahu.

Druhým způsobem je určení kritické části stanoveného rozsahu ve spojitosti s konkrétními nepominutelnými funkcemi stanovenými v příloze k prováděcímu právnímu předpisu (dále jen „příloha“). Pokud aktiva stanoveného rozsahu zajišťují takto stanovené nepominutelné funkce, jedná se o kritickou součást stanoveného rozsahu. Zákon zmocňuje v § 27 odst. 4 vládu vydat nařízení, ve kterém nepominutelné funkce stanoví.

Návrh nařízení vlády o nepominutelných funkcích stanoveného rozsahu (dále jen „návrh nařízení“) byl původně odrazem pouze druhého ze shora uvedených způsobů. Po úpravě znění návrhu nařízení na základě politické dohody, která proběhla na jednání Výboru pro bezpečnost Poslanecké sněmovny Parlamentu České republiky (dále jen „ČR“) dne 3. dubna 2025, byl návrh nařízení rozšířen také o první, subjektivní, způsob určení kritické části stanoveného rozsahu. Na základě této dohody došlo k přesunu aktiv stanoveného rozsahu, u kterých byl poskytovatelem regulované služby v režimu vyšších povinností (na kterého dopadají povinnosti z mechanismu posuzování dodavatelů) ohodnocen dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká (dále jen „vysoká aktiva“), ze zákona do návrhu nařízení. Účelem návrhu nařízení, z hlediska objektivního přístupu, je stanovit a konkretizovat nepominutelné funkce, aby byla objektivně stanovena množina aktiv, které jsou natolik

významné, že dodavatelé, kteří poskytují plnění do těchto funkcí, musí podléhat mechanismu posuzování dodavatelů.

Vzhledem k dynamickému vývoji moderních technologií a potřebě kvalifikovaného stanovení nepominutelných funkcí je třeba velmi pečlivě a s rozvahou identifikovat, jaké funkce budou do této množiny spadat. Ačkoliv je vůlí normotvůrce vymezení těchto funkcí v rámci jednoho prováděcího právního předpisu, je zřejmé, že identifikace všech funkcí, jež by měly být identifikovány jako nepominutelné, je časově a kapacitně velmi náročná a vyžaduje značnou odbornost. Vydání takto celistvého nařízení vlády současně s přijetím zákona nebo krátce poté nelze reálně očekávat.

Současně je ale zřejmé, že bez dostatečně rychlého vydání prováděcího právního předpisu, který by stanovil nepominutelné funkce, bude aktivace mechanismu posuzování dodavatelů závislá pouze na subjektivním způsobu určení kritické části stanoveného rozsahu, jak je ve stručnosti uvedeno výše. Takový stav by byl dlouhodobě velmi neuspokojivý, jelikož by mohlo docházet k rozdílným přístupům i kvalitě provedení identifikace kritických aktiv jednotlivými poskytovateli regulovaných služeb. Jako kritická by nemusela být ohodnocena všechna aktiva, na nichž bude poskytování regulované služby vždy vysoce závislé. Ve vztahu k takovým aktivům by pak docházelo i k rozdílnému způsobu aplikace zmírňování rizik spojených s dodavateli. Tento stav by nebyl v souladu s bezpečnostními zájmy státu.

S ohledem na velmi závažný dopad mechanismu posuzování dodavatelů je proto nezbytné, aby vláda určovala nepominutelné funkce jednotlivých regulovaných systémů, a to v případě, není-li pochyb o kritičnosti nebo vysoké důležitosti aktiv, která tyto funkce pro poskytování regulované služby zajišťují. Cílem právní úpravy je vymezení takových funkcí, jejichž významnost je nezpochybnitelná, protože na nich bude poskytování regulované služby vždy vysoce závislé. Oblastí, na kterou dopadá navrhovaný rozsah nařízení vlády, jsou všechny strategicky významné služby v § 2 tohoto návrhu nařízení a sektor elektronických komunikací, kterému je věnován § 3. Jedná se o technologickou oblast, pro kterou mají informační a komunikační technologie (dále jen „ICT“) klíčový význam, a která je vnitrostátně i mezinárodně vysoce standardizovaná. V ČR je tato oblast rovněž specificky regulována zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, který zřizuje Český telekomunikační úřad, který na dodržování regulace dohlíží. Stát má proto dostatečné kapacity, aby mohl odpovědným způsobem autoritativně určit nepominutelné funkce elektronických komunikací, a to včetně dosud plně nezavedených sítí 5. generace (dále také „5G“).

K obdobnému vymezení tzv. kritických funkcí pro sektor elektronických komunikací přistoupilo i mnoho dalších států včetně členských států Evropské unie (dále jen „EU“), jako je Francie, Německo a Finsko, ale i Spojené království, které členem EU již není. Přehled kritických funkcí sítí elektronických komunikací zveřejnila jako součást Souboru opatření EU pro kybernetickou bezpečnost sítí 5G (dále jen „EU 5G Toolbox“) také Skupina pro spolupráci (tzv. NIS Cooperation Group).

EU 5G Toolbox[1] označuje za kritické funkce 5G sítí funkce spojené s jádrem sítě (tzv. core network functions), funkce správy a síťové orchestrace (dále také „MANO“). Za vysoce důležitou funkci je považována funkce přístupu k radiové síti (dále také „RAN“). Za středně nebo vysoce důležité jsou dále považovány funkce ostatních systémů řízení a podpůrných služeb kromě MANO, transportní a přenosové funkce a funkce internetwork exchanges.

Obdobně k hodnocení kritičnosti funkcí 5G sítí přistupuje také německý regulátor sektoru elektronických komunikací Bundesnetzagentur (dále také „BNetzA“). BNetzA do seznamu kritických funkcí[2] zařadil všechny funkce popsané v EU 5G Toolboxu, tedy funkce spojené s jádrem sítě, funkce ostatních systémů řízení a podpůrných služeb včetně funkce MANO, transportní a přenosové funkce a funkce internetwork exchanges.

Také Národní centrum kybernetické bezpečnosti Spojeného království (dále jen „NCSC“) vydalo doporučení pro vymezení rozsahu sítí 5G, 4G i sítí elektronických komunikací obecně. Toto vymezení specifikuje části sítí, kde přítomnost tzv. vysoce rizikového dodavatele[3] nelze mitigovat technickými opatřeními. Jedná se o vymezení částí sítí elektronických komunikací, kde by zařízení vysoce rizikových dodavatelů neměla být vůbec využívána. Toto vymezení funkcí je poměrně podrobně popsáno v Doporučení NCSC pro využívání zařízení vysoce rizikových dodavatelů v telekomunikačních sítích Spojeného království.[4]

Francie v Kodexu poštovní a elektronické komunikace (Code des postes et des communications électroniques)[5] specifikuje zařízení, resp. funkce 5G sítí, jejichž pořízení podléhá udělení povolení ze strany státu. V případě francouzské regulace se jedná o specifikaci funkcí podle standardů 3GPP pro 5G sítě, konkrétně do této kategorie spadají funkce New Radio Base Station (en-gNodeB a gNodeB), Access and Mobility management Function (AMF), Authentication Server Function (AUSF), User Plane Function (UPF), Session Management Function (SMF), Policy Control Function (PCF), Network Slice Selection Function (NSSF), Network Repository Function (NRF), Network Exposure Function (NEF), Unified Data Management (UDM) a Security Edge Protection Proxy (SEPP).

Velmi podrobně vymezené kritické části sítě elektronických komunikací má také Finsko. Finská dopravní a komunikační agentura TRAFICOM vymezuje zejména kritické funkce 4G sítí, 5G sítí i sítí elektronických komunikací obecně.[6] Do tohoto výčtu zahrnuje úžeji vymezené funkce než např. Německo nebo Skupina pro spolupráci v EU 5G Toolboxu.

Návrh nařízení předkládá vláda na základě zmocnění uvedeném v § 27 odst. 4 zákona.

[1] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468, str. 29-40.

[2] Katalog der Sicherheitsanforderungen (bundesnetzagentur.de), str. 4.

[3] Vysoce rizikový dodavatel z pohledu NCSC je specifikován v Doporučení NCSC pro využívání zařízení vysoce rizikových dodavatelů v telekomunikačních sítích Spojeného království. Dostupné zde: NCSC advice on high risk vendors in UK telecoms - NCSC.GOV.UK

[4] NCSC advice on high risk vendors in UK telecoms - NCSC.GOV.UK

[5] Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques - Légifrance (legifrance.gouv.fr)

[6] Regulation on critical parts of a communications network

## 2. Zhodnocení platného právního stavu

Oblast stanovení nepominutelných funkcí stanoveného rozsahu pro strategicky významné služby z hlediska kybernetické bezpečnosti dosud nebyla nijak komplexně regulována. Předkládaný návrh úpravy obsažený v nařízení vlády tudíž představuje novou regulaci reflektující požadavek Bezpečnostní rady státu k vytvoření tzv. mechanismu prověřování bezpečnosti dodavatelského řetězcem které navazuje na vývoj na poli kybernetických bezpečnostních hrozeb a nutnost na ně ze strany státu přiměřeně reagovat.

Stanovení seznamu nepominutelných funkcí stanoveného rozsahu pro strategicky významné služby podle tohoto návrhu nařízení pak představuje národní úpravu respektující požadavek Bezpečnostní rady státu v souladu s materiálem „Bezpečnost dodavatelských řetězců strategické infrastruktury státu“, č. j. 28261/2022-UVCR, jejž Bezpečnostní rada státu vzala na vědomí svým usnesením č. 41 ze dne 21. června 2022.

## 3. Zhodnocení souladu návrhu právního předpisu s ústavním pořádkem a ostatními součástmi právního řádu České republiky

Návrh nařízení je v souladu s ústavním pořádkem ČR.

Jako prováděcí právní předpis odráží soulad zákona s ústavním pořádkem. Navrhovaná právní regulace kybernetické bezpečnosti se dotýká především práva vlastnického a částečně též i z něj odvozovaného práva na svobodu podnikání podle Listiny základních práv a svobod. Povinnosti, které navrhovaná právní úprava stanoví vybraným subjektům (tzv. poskytovatelům regulované služby), totiž v různé míře omezují tyto subjekty v možnosti neomezeně užívat systémy, k nimž vykonávají vlastnická nebo obdobná práva.

Zákonná právní úprava v rámci těchto práv omezuje povinné subjekty v zásadě plošně. Plošné omezení vlastnického práva, resp. práva na podnikání, má v tomto případě formu zavedení povinností, zejména implementovat bezpečnostní opatření, hlásit kybernetické bezpečnostní incidenty a provádět vydaná protiopatření. Úzké části poskytovatelů regulované služby s potenciálně největšími dopady pro fungování ČR může také omezit vlastnické právo, resp. právo na podnikání, v rámci nově zaváděného mechanismu posuzování dodavatelů.

Zákon, na který obsahově navazuje tento návrh nařízení, se vypořádal s odůvodněním narušení výše uvedených práv následovně:

S ohledem jak na zájmy bezpečnostní, tak i ekonomické, je stanovení nepominutelných funkcí orientováno na minimalistický přístup, jehož podstatou je podřadit pod regulaci návrhu zákona prvky vyžadující ochranu, nicméně nepřekračovat a neregulovat subjekty v ČR plošně. Možné omezení práva na užívání majetku, za které by snad povinná bezpečnostní opatření uložená tímto Zákonem a jeho budoucími prováděcími předpisy mohla být považována, má za účel chránit obecné zájmy, kterými je bezpečnost státu a obyvatelstva či významné ekonomické a společenské zájmy. Kybernetická bezpečnost ČR jako podmnožina bezpečnosti ČR spadá do rozsahu působnosti ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR, ve znění ústavního zákona č. 300/2000 Sb. Podle čl. 1 uvedeného ústavního zákona je zajištění svrchovanosti a územní celistvosti ČR, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu. Návrh zákona lze považovat za jeden z prostředků plnění této povinnosti státu. Návrh zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu rozvoje digitální společnosti a ekonomiky, o nějž ČR jako členský stát EU usiluje.

K zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě konstatovat, že předkládaný návrh zákona je také v tomto směru v souladu s ústavním pořádkem ČR.

Zavedení uvedeného mechanismu je v souladu s článkem 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústava ČR, který stanovuje, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon, s článkem 41 odst. 2 Ústavy, podle kterého má vláda právo zákonodárné iniciativy, a článkem 79 odst. 1 Ústavy, podle kterého lze působnost správních orgánů stanovit pouze zákonem.

Navrhovaný způsob posuzování dodavatelů je rovněž v souladu s čl. 2 odst. 2 Listiny, podle kterého lze státní moc uplatňovat jen v případech a mezích stanovených zákonem, a to způsobem, který zákon stanoví, článek 4 odst. 1 Listiny, podle kterého mohou být ukládány povinnosti toliko na základě zákona a v jeho mezích a jen při zachování lidských práv a svobod, a článek 2 odst. 3 Listiny, podle kterého každý může činit, co není zákonem zakázáno, a nikdo nemůže být nucen činit, co zákon neukládá.

Listina upravuje možnost omezení některých práv v ní zakotvených, konkrétně v případě předkládaného návrhu zákona práva podnikat stanoveného článkem 26 odst. 1 Listiny nebo práva na ochranu dobré pověsti stanového v článku 10 odst. 1 Listiny. Obecně platí, že některá základní práva mohou být podle Listiny omezena. Omezení musí být ovšem stanovena zákonem, musí být v souladu s Listinou a musí být založena na jejich potřebnosti k dosažení legitimních společenských cílů, jako je např. zabezpečení existence státu, ochrany jeho demokratické povahy, zachování veřejného zdraví a pořádku (srov. např. usnesení Ústavního soudu ze dne 19. 3. 2009, sp. zn. IV. ÚS 266/09-1 či usnesení Ústavního soudu ze dne 7. 3. 2014, sp. zn. I. ÚS 110/14-1). Při posuzování souladu těchto omezení s ústavním pořádkem je uplatňován princip proporcionality, kdy jsou aplikována kritéria vhodnosti, potřebnosti a poměřování (srov. nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94).

V případě prověřování bezpečnosti dodavatelského řetězce je takovýmto legitimním cílem ochrana bezpečnosti státu a vnitřního pořádku, v jejímž rámci stát v souladu s čl. 4 odst. 2 ve spojení s čl. 26 odst. 2 Listiny stanoví omezení pro výkon určitých činností, a tím omezí právo podnikat a provozovat jinou hospodářskou činnost, které je zakotveno v čl. 26 odst. 1 Listiny. Obdobné lze říci i o právu na ochranu dobré pověsti, které náleží i právnickým osobám (srov. např. rozsudek Nejvyššího soudu ze dne 14. 3. 2018, sp. zn. 23 Cdo 5173/2017 či nález Ústavního soudu ze dne 10. 10. 2001, sp. zn. I. ÚS 201/01), a které může být procesem prověřování bezpečnosti dodavatelského řetězce dotčeno. Případné omezení těchto práv je proto v souladu s ústavním pořádkem ČR.

Článek 11 odst. 4 Listiny stanoví, že vyvlastnění nebo nucené omezení vlastnického práva je možné ve veřejném zájmu, a to na základě zákona a za náhradu. Předkládaný návrh může omezit možnost provozovatelů strategicky významné infrastruktury svobodně nakládat se svým majetkem, ale k takovému omezení dochází při uplatnění principu proporcionality vůči ochraně veřejného zájmu ve formě zvyšování bezpečnosti státu. Minimalizaci zásahu do vlastnictví povinných osob zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů.

## 4. Zhodnocení souladu návrhu právního předpisu se závazky vyplývajícími pro Českou republiku z jejího členství v Evropské unii

Návrh nařízení nezapracovává do právního řádu ČR předpisy EU a není s nimi v rozporu. Daná oblast není dotčena judikaturou soudních orgánů EU a je v souladu s obecnými právními zásadami práva EU. Na základě těchto skutečností je možné návrh nařízení hodnotit jako plně slučitelný s právem EU. Znění návrhu nařízení vychází z přístupů k chráněným nebo nepominutelným funkcím dalších členských států EU. V rámci mezinárodní spolupráce provedl Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) sérii bilaterálních jednání[1] určených k seznámení se s jednotlivými národními přístupy, které proběhly především v průběhu roku 2022.

Obsah tohoto návrhu nařízení nemá žádný vztah k obsahu nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013, tzv. „aktu o kybernetické bezpečnosti“.

Návrh nařízení byl rovněž posouzen z hlediska souladu se směrnicí Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

Návrh nařízení je v souladu s obecnými zásadami práva Evropské unie, jako jsou např. zásada právní jistoty, proporcionality a zákaz diskriminace.

Návrh nařízení není v rozporu s judikaturou soudních orgánů Evropské unie a je v souladu s obecnými zásadami práva Evropské unie (např. zásadou právní jistoty, proporcionality a zákazem diskriminace)

Na základě těchto skutečností je možné návrh nařízení hodnotit jako plně slučitelný s právem Evropské unie.

[1] Německo, Velká Británie.

## 5. Zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami, jimiž je Česká republika vázána

Na mezinárodním poli neexistuje mezinárodní smlouva, která by upravovala problematiku kybernetické bezpečnosti, co se týče návrhu tohoto nařízení, zde jsou pro vyhodnocení relevantní zejména dohody týkající se mezinárodního obchodu, s čímž se důvodová zpráva k samotnému návrhu zákona vyrovnala následujícím způsobem:

Předkládaný návrh je v souladu rovněž s výjimkami smluv inkorporovaných do Dohody o zřízení Světové obchodní organizace. Jejich společným cílem je zamezení vytváření bariér mezinárodního obchodu a vzájemná doložka nejvyšších výhod, tzn. povinnost zacházet s investory a dodavateli smluvních stran ne méně příznivě než se subjekty třetích států. Předkládaný návrh má potenciál omezit zacházení s dodavateli některých smluvních stran na úroveň méně příznivou ve srovnání se zacházením s dodavateli ze třetích států, ale dochází tak v rámci níže uvedených povolených výjimek.

Všeobecná dohoda o clech a obchodu 1994 (GATT) připouští v čl. XX opatření omezující mezinárodní obchod za předpokladu jejich nutnosti a) k ochraně života a zdraví lidí, nebo d) zachování zákonů a jiných předpisů, které nejsou neslučitelné s jejími ustanoveními. Všeobecná dohoda o obchodu službami (GATS) v čl. XIV upravuje výjimky obdobně jako GATT, přičemž opatření k zabezpečení shody s právními předpisy doplňuje demonstrativní výčet explicitně zmiňující bezpečnostní předpisy (čl. XIV písm. c) bod (iii)).

Omezení mezinárodního obchodu předkládaným návrhem zákona je plně v souladu s výjimkami GATT i GATS, a proto neodporuje závazkům ČR přijatým v rámci Světové obchodní organizace.

Uvedené skutečnosti se rovněž aplikují ve vztahu k bezpečnosti dodavatelského řetězce. V kontextu této problematiky Úřad provedl průzkum a konzultace u zahraničních partnerů Úřadu, jako jsou analogie Úřadu ze Spojeného království či Německa. Uvedené země již obdobným mechanismem disponují, přičemž gestoři mechanismů neshledávají rozpor mezi fungováním vlastního mechanismu bezpečnosti dodavatelského řetězce, směřujícímu k ochraně bezpečnosti a veřejného pořádku, a smyslem smluv GATT či GATS, jakožto závazcích těchto zemí přijatých na plénu Světové obchodní organizace.

V rámci mechanismu by měly být uplatněny výjimky v případě limitování nebo zákazu dodavatele, zejména ve smyslu čl. XIV GATS a čl. XX GATT a také ve smyslu čl. XIVbis GATS a čl. XXI GATT. Nástroje mechanismu bezpečnosti dodavatelského řetězce se vztahují pouze na nejkritičtější infrastrukturu, jejíž narušení má schopnost narušit jak veřejný pořádek či veřejnou morálku ve smyslu č. XIV GATS a XX GATT, tak také ohrozit bezpečnost státu, což spadá pod čl. XIVbis GATS a čl. XXI GATT.

Navrhovaná právní úprava je dále v souladu s bilaterálními dohodami o podpoře a ochraně investic. Dohody o ochraně investic zavazují ČR k tomu, aby poskytovala ochranu investorům pocházejícím z jiných smluvních států a jejich investicím v ČR. Jednou z podmínek zakotvených ve valné většině bilaterálních dohod o podpoře a ochraně investic, která určuje, zda je zahraniční investice chráněnou investicí, je soulad hospodářských aktivit investora s vnitrostátními předpisy druhé smluvní strany.

Předkládaný návrh vytváří právní rámec především pro budoucí investice, kladení nových nároků na dodavatele tudíž není v rozporu s uvedeným.

Ochrana stávajících investic podle bilaterálních dohod o podpoře a ochraně investic taktéž není narušena, neboť návrh respektuje životní cyklus produktů, proto nevytváří nadbytečné náklady spojené s již uskutečněnou investicí. Dostatečná lhůta navíc umožňuje investorům se na nové právní podmínky adaptovat, jak změnou dodavatelů, tak snížením vlastní rizikovosti investorů, jejíž kritéria jsou součástí předkládaného návrhu zákona. Jedná se tudíž o minimální možný zásah k dosažení účelu předkládaného návrhu zákona, zajištění bezpečnosti dodavatelského řetězce strategicky významné infrastruktury. V neposlední řadě obsahuje většina bilaterálních dohod o podpoře a ochraně investic doložku se základními bezpečnostními zájmy smluvních stran. Doložka opravňuje strany přijmout taková opatření, která považují za nezbytná pro ochranu svých základních bezpečnostních zájmů. Ochrana nejvýznamnější kritické infrastruktury nezbytné pro fungování státu se řadí pod základní bezpečnostní zájem státu, tudíž lze případná omezení vyplývající z aplikace předkládaného návrhu podřadit pod skutkovou podstatu uvedené výjimky.

Bilaterální dohody o podpoře a ochraně investic také řadí mezi základní bezpečnostní zájmy smluvní strany ty zájmy, které vyplývají z jejího členství v celní, hospodářské nebo měnové unii, volném trhu nebo zóně volného obchodu. Směrnice NIS 2 ukládá členským státům, aby zajistily přijetí opatření k řízení bezpečnostních rizik sítí a informačních systému, přičemž bezpečnost dodavatelského řetězce zmiňuje v čl. 21 odst. 2. písm. d) v demonstrativním výčtu minima nutných opatření. Návrh právní úpravy mechanismu prověřování bezpečnosti dodavatelského řetězce tedy není v rozporu s bilaterálními dohodami o ochraně investic, jimiž je Česká republika vázána.

## 6. Zhodnocení, zda návrh právního předpisu neobsahuje ustanovení, které by bylo svou povahou technickým předpisem podle právního předpisu upravujícího technické požadavky na výrobky

Ustanovení návrhu tohoto nařízení obsahují pouze vymezení seznamu nepominutelných funkcí stanoveného rozsahu pro strategicky významné služby, žádné technické požadavky na výrobky toto nařízení neobsahuje.

## 7. Informace o splnění oznamovací povinnosti podle tohoto právního předpisu (ve vztahu k ne/obsaženým ustanovením, která by byla svou povahou technickým předpisem podle právního předpisu upravujícího technické požadavky na výrobky)

Vzhledem k posouzení dle bodu 6 oznamovací povinnost nevznikla.

## 8. Informace o konzultaci návrhu právního předpisu s Evropskou centrální bankou a výsledku konzultace, podléhá-li návrh právního předpisu takové konzultaci

Návrh nařízení nemá vliv na měnovou politiku Evropské unie, tedy nepodléhá konzultaci s Evropskou centrální bankou.

## 9. Předpokládaný hospodářský a finanční dopad návrhu právního předpisu na státní rozpočet a ostatní veřejné rozpočty

Samotný návrh nařízení dopad na státní rozpočet ani ostatní veřejné rozpočty nemá, dopady vyvolává zákon, k jehož provedení je vydáváno. Zvýšení zabezpečení u organizací naplňujících kritéria založená zákonem a stanovená tímto návrhem nařízení bude mít finanční dopady vyčíslené v rámci důvodové

zprávy k zákonu, každopádně však přispěje k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí.

Stanovení seznamu nepominutelných funkcí stanoveného rozsahu přímo ovlivňuje to, jakým typům organizací a kolika takovým organizacím budou aktivovány zákonem předpokládané povinnosti týkající se strategicky významných služeb, konkrétně zapojení se do mechanismu prověřování bezpečnosti dodavatelského řetězce.

V otázce vyčíslení nákladů na zapojení se do mechanismu prověřování bezpečnosti dodavatelského řetězce lze odkázat plně na důvodovou zprávu k zákonu – důvodová zpráva a hodnocení dopadů regulace byly k tomuto tématu zpracovány již v první verzi návrhu zákona do mezirezortního připomínkového řízení a následně byly ještě dále na základě požadavků doplňovány. Zkráceně je možno uvést, že náklady přímo spojené s plněním této povinnosti jsou dány v rozsahu administrativní zátěže, která bude provedena přímo v souvislosti s vynaložením přiměřeného úsilí při zjišťování informací o dodavatelích bezpečnostně významných dodávek a evidencí a hlášením těchto informací ve smyslu § 31 návrhu zákona. Další případné náklady případně může generovat omezení rizik spojených s dodavatelem, pokud bude takové omezení vydáno – toto je však již předmětem aplikace daného mechanismu na danou situaci a jako takové je toto posuzováno v okamžiku vydávání daného konkrétního opatření.

## 10. Předpokládaný dopad návrhu právního předpisu na práva a povinnosti fyzických a právnických osob

Navrhovaná právní úprava nezakládá fyzickým a právnickým osobám žádná nová práva ani povinnosti. Práva a povinnosti jsou upraveny v zákoně, který zmocňuje k vydání tohoto návrhu nařízení. Návrh nařízení představuje návrh prováděcího právního předpisu, na jehož základě vzhledem k jeho povaze nemohou být ukládány povinnosti ani vznikat nová práva.

## 11. Předpokládaný dopad návrhu právního předpisu na podnikatelské prostředí České republiky

Samotný návrh nařízení nemá na podnikatelské prostředí žádný vliv, neboť takovéto dopady vyvolává výhradně zákon, k jehož provedení je tento návrh nařízení vydáván. Hodnocení dopadů návrhu zákona na podnikatelské prostředí je podrobně rozvedeno v rámci hodnocení dopadů zákona.

## 12. Předpokládaný sociální dopad návrhu právního předpisu, včetně dopadu na specifické skupiny obyvatel, především na osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny

Návrh nařízení je z hlediska sociálních dopadů a dopadů na specifické skupiny obyvatel neutrální. Zvýšení úrovně kybernetické bezpečnosti, a tím pádem zajištění regulovaných služeb bude mít druhotný pozitivní dopad na společenské a ekonomické činnosti jako např. zajištění zdravotní péče či dodávky energie. Návrh nařízení je rovněž neutrální z hlediska dopadů na životní prostředí, lze však obdobně předpokládat pozitivní efekt v podobě předcházení takových bezpečnostních incidentů, které by negativní dopad mohly mít.

## 13. Předpokládaný dopad návrhu právního předpisu na rovnost mužů a žen, upravuje-li návrh právního předpisu postavení fyzických osob nebo se tohoto postavení dotýká

Navrhovaná právní úprava je z hlediska zákazu diskriminace a z hlediska rovnosti mužů a žen neutrální.

## 14. Předpokládaný dopad návrhu právního předpisu na životní prostředí

Návrh nařízení nemá specifický dopad na životní prostředí.

## 15. Předpokládaný dopad návrhu právního předpisu na ochranu práv dětí

Návrh nařízení nemá specifický dopad na ochranu práv dětí.

## 16. Předpokládaný dopad návrhu právního předpisu na bezpečnost nebo obranu státu

Vzhledem k povaze navrhovaných změn lze konstatovat, že návrh nařízení má velmi pozitivní dopady na bezpečnost a obranu státu. Určením nepominutelných funkcí se zajistí ochrana kritických částí systémů regulovaných subjektů v důsledku čehož dojde k navýšení úrovně kybernetické bezpečnosti, odolnosti strategické infrastruktury a stability služeb v ČR.

Ochrana nepominutelných funkcí může mít s ohledem na její povahu v návrhu nařízení pozitivní dopad na bezpečnost a obranu státu, zejména díky schopnosti centralizovat a vyhodnocovat informace o bezpečnostních hrozbách a zranitelnostech z celého světa ve vztahu k těmto funkcím a na základě toho přijímat potřebné kroky dříve a ve vyšší kvalitě.

Dále dojde k aplikaci povinností plynoucích z mechanismu posuzování dodavatelů napříč povinnými osobami mechanismu obdobným způsobem, a to zejména tím, že funkce, jejichž významnost je nezpochybnitelná a jež jsou zajišťovány aktivy, která by měla být vždy ohodnocena jako vysoká nebo kritická, protože na nich bude poskytování regulované služby vždy vysoce závislé, budou pevně stanoveny. Stanovením konkrétních nepominutelných funkcí dojde ke zmírnění rozdílného přístupu k provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb, a tedy i rozdílnému způsobu aplikace zmírňování rizik spojených s dodavateli vztahujícímu se k těmto aktivům, což bude mít pozitivní vliv na bezpečnost státu.

## 17. Zhodnocení dopadu návrhu právního předpisu ve vztahu k ochraně soukromí a osobních údajů

Návrh nařízení se netýká soukromí.

## 18. Zhodnocení, zda návrhem právního předpisu není zakládána veřejná podpora

Navrhovanou právní úpravou není zakládána veřejná podpora. Veřejná podpora je termín vycházející ze Smlouvy o fungování EU, kdy se jí rozumí každá podpora poskytnutá v jakékoli formě státem nebo z veřejných prostředků, která narušuje nebo může narušit hospodářskou soutěž tím, že zvýhodňuje určité podniky nebo určitá odvětví výroby a ovlivňuje obchod mezi členskými státy. Podpora, která splňuje uvedená kritéria, je neslučitelná se společným trhem EU, a tedy zakázaná. Návrh nařízení nepracuje s rozdělováním veřejných prostředků, neobsahuje přímé nebo nepřímé zvýhodnění určitých podniků či odvětví a nemá selektivní charakter.

## 19. Zhodnocení korupčních rizik návrhu právního předpisu

V této oblasti nebyla shledána žádná nová vazba ani nová rizika. Právě naopak, zkonkretizování nepominutelných funkcí má snahu zamezit případnému rozdílnému přístupu i kvalitě provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb, a tedy i k rozdílnému způsobu aplikace zmírňování rizik spojených s dodavateli vztahujícímu se k těmto aktivům

**20. Odůvodnění případného návrhu, aby Poslanecká sněmovna vyslovila s návrhem právního předpisu souhlas již v prvém čtení (pokud se navrhuje)**

Nařízení vlády neprojednává Poslanecká sněmovna.

**21. Odůvodnění případného návrhu, aby navrhovaná právní úprava nabyla účinnosti dříve než počátkem patnáctého dne následujícího po dni jejího vyhlášení (pokud se navrhuje)**

Nenavrhuje se.

**22. Odůvodnění odchylek v postupu projednání návrhu právního předpisu (pokud se navrhují a jsou odlišné od předchozích) (jsou-li navrhovány, může být konzumováno předchozími kapitolami)**

Nejsou navrhovány žádné odchylky v postupu projednávání návrhu právního předpisu.

# II. Zvláštní část

## K Celé Nařízení vlády

### K § 1

Smyslem daného ustanovení je vymezení předmětu regulace navrhovaného nařízení a odkázání na zmocňovací ustanovení návrhu zákona, na základě něhož je prováděcí právní předpis vydáván.

### K § 2

Pro potřeby návrhu nařízení odpovídají nepominutelné funkce stanovené seznamem nepominutelných funkcí vysokým aktivům podle hodnocení aktiv podle přílohy č. 2 k vyhlášce č. XX/XXXX Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Tato vysoká aktiva zahrnují činnosti nebo vlastnosti, jejichž narušení může mít závažný dopad na poskytování strategicky významné služby ve smyslu § 27 odst. 3 zákona a naplňují tak zákonnou definici nepominutelné funkce.

Vysoká aktiva jsou velmi důležitá až kritická pro fungování strategicky významných služeb. Tato aktiva mají podstatné dopady na primární aktiva, a tudíž i na chod celé strategicky významné služby a mohou zásadně ovlivnit její dostupnost, zajištění důvěrnosti nebo integrity.

Znění zákona, na základě něhož je tento prováděcí právní předpis vydáván, před úpravou vycházející z pozměňovacích návrhů schválených Poslaneckou sněmovnou Parlamentu ČR obsahovalo v kritické části stanoveného rozsahu strategicky významných služeb také vysoká aktiva. Na základě politické dohody, která proběhla na jednání Výboru pro bezpečnost Poslanecké sněmovny Parlamentu ČR dne 3. dubna 2025, však byla vysoká aktiva ze zákona odstraněna a bylo dohodnuto, že budou obsažena v nařízení o nepominutelných funkcích jako nepominutelné funkce.

### K § 3

Nepominutelné funkce pro služby zajišťování veřejné komunikační sítě a poskytování veřejně dostupné služby elektronických komunikací jsou vymezeny dvojím způsobem.

Stejně jako nepominutelné funkce stanoveného rozsahu ostatních strategicky významných služeb jsou představovány vysokými aktivy podle hodnocení aktiv podle přílohy č. 2 k vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Dále jsou také vymezeny seznamem nepominutelných funkcí služeb zajišťování veřejné komunikační sítě a poskytování veřejně dostupné služby elektronických komunikací obsaženým v příloze, která tyto funkce blíže specifikuje pro jejich identifikaci v jednotlivých architekturách veřejných komunikačních sítí.

## K § 4

Zákon a návrh nařízení jsou vzájemně komplementární. Je v zájmu jak normotvůrce, tak adresátů prováděcího právního předpisu, aby zákon a nařízení vstoupily v účinnost ve stejný okamžik. Jelikož zákon, k jehož provedení se nařízení vydává, nemá k okamžiku zahájení meziresortního připomínkového řízení známý pevný okamžik nabytí účinnosti, tak termín účinnosti návrhu nařízení byl po konzultaci se Sbírkou zákonů orientačně dán na datum, které umožňuje zahájit v systému eLegislativa meziresortní připomínkové řízení, nicméně i nadále se počítá s úpravou účinnosti nařízení podle účinnosti zákona.

## K označení přílohy příloha

Příloha obsahuje seznam specifikující nepominutelné funkce veřejných komunikačních sítí, zejména ve formě softwarových či hardwarových komponent a prvků, jež jsou podle níže popsaných technických specifikací považovány za kritické, tudíž pro účely návrhu nařízení a bezpečnost dodavatelského řetězce nepominutelné, a to jak pro veřejné komunikační sítě obecně, tak specificky pro 5. a 4. generaci mobilní veřejné komunikační sítě (dále také „5. generace sítí“ a „4. generace sítí“). Uvedené 5. a 4. generace sítí jsou z hlediska prostředí veřejných komunikačních sítí velmi rozšířené a zároveň standardizované na velmi vysoké, sektorem elektronických komunikací uznávané, úrovni kvality. Seznam uvedený v příloze se tudíž sestává jak z univerzálně používaných názvů jednotlivých funkcí, které jsou z důvodu sjednocené praxe v oboru ICT uvedeny v anglickém jazyce, včetně rozšířených zavedených zkratek, tak z jejich věcného popisu pro upřesnění úlohy těchto funkcí.

Tyto funkce byly převážně extrahovány z technických specifikací 3GPP TS 23.501

a 3GPP TS 23.002, jejichž kritický význam vyplývá nejen ze samotných technických specifikací, ale i z jejich užití v rámci ochrany kritických částí veřejných komunikačních sítí Spojeného království, Francie, Finska nebo Německa. Jako inspirace pro stanovení nepominutelných funkcí tohoto návrhu nařízení posloužily zejména regulace obdobných funkcí ve Finsku, Spojeném království, Francii a Německu.

Příloha nejprve stanovuje funkce veřejných komunikačních sítí v obecném pojetí tak, aby toto pojetí dopadalo na veškeré sítě veřejných komunikací, včetně 2., 4. či 5. generace sítí a ostatní síťové služby jako je například tzv. IP Multimedia Subsystem, zkráceně IMS podle technických specifikací 3GPP TS 23.228. Smysl takového rozdělení je dvojí. Jednak je určen rozsah, na který se uplatní konkrétní funkce spadající pod 4. a 5. generaci sítí, jak jsou dále popsány v příloze návrhu nařízení, jednak takové obecné pojetí představuje vodítko pro určení nepominutelných funkcí, které nelze podřadit pod žádné technologické standardy nebo které jsou méně rozšířené či se nachází ve vývoji.

## K označení přílohy příloha

Ad 1. Nepominutelné funkce ve veřejné komunikační síti související s řízením síťových zdrojů, se směrováním a jinou kontrolou nebo řízením provozu koncových uživatelů ve veřejné komunikační síti, které mohou mít významný dopad na síťový provoz.

První část přílohy definuje síťové funkce ve veřejné komunikační síti, které musí být považovány za kritickou část veřejné komunikační sítě, a tedy pro potřeby návrhu nařízení za funkce nepominutelné.

Seznam je technologicky neutrální z důvodu úpravy funkcí pro jednotlivé technologie a služby fungující napříč veřejnými komunikačními sítěmi. Z hlediska bezpečnosti pro funkce uvedené v první části přílohy platí, že tyto funkce nemusí být realizovány v plném rozsahu svých možností, ale k jejich zařazení do množiny nepominutelných funkcí ve smyslu návrhu nařízení postačí částečná realizace těchto funkcí v síťové infrastruktuře. Navíc platí, že jednotlivé softwarové komponenty, síťová zařízení nebo služby mohou jak podporovat část těchto nepominutelných funkcí, tak také více funkcí na jedné komponentě.

Mezi nepominutelné funkce patří rovněž ty, které slouží pro služby nebo komponenty s rozsáhlým pokrytím nebo vysokým počtem uživatelů. Za kritickou lze považovat například infrastrukturu, která pokrývá více než 30 000 km² území ČR (tj. přibližně 40 % rozlohy), slouží více než 100 000 uživatelům u základních služeb (např. telefonie, SMS, internet), dosahuje více než 500 000 uživatelů u služeb masové komunikace (např. rozhlas, televizní vysílání), nebo obsluhuje více než 300 000-400 000 uživatelů v případě e-mailových a jiných služeb digitální komunikace. Tyto hranice jsou orientační a mají za cíl postihnout případy, kdy by výpadek dané funkce mohl mít zásadní dopad na dostupnost, bezpečnost nebo stabilitu elektronických komunikací v ČR. Při hodnocení je třeba brát v úvahu také míru závislosti dalších služeb na dané infrastruktuře.

Kromě toho se tyto funkce vztahují na systémy, jež jsou schopné analyzovat uživatelský provoz, a které se používají k odhalování nežádoucího, popř. škodlivého, síťového provozu a které mohou být rovněž zahrnuty do funkcí sloužících k zabezpečení informací. Tyto typy funkcí jsou obvykle implementovány v tzv. jádru sítě, neboli páteřní síti, což je taková část sítě, kterou lze na základě jejího specifického rozhraní oddělit od okrajové části sítě.

V případě mobilních sítí se tento odstavec vztahuje zejména na funkce související s přenosem uživatelské roviny nebo používané k řízení síťového provozu prostřednictvím řídicí roviny, s čímž souvisí řízení mobility v mobilní síti.

Obecně se tyto funkce používají k řízení a správě síťového provozu, a proto je třeba je považovat za kritické části sítě elektronických komunikací, a tedy nepominutelnou funkci veřejné komunikační sítě. Tyto funkce rovněž hrají významnou roli při zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti komunikační sítě jako celku.

Ad číslo 1.1

Toto číslo obsahující zejména evidenci, správu přístupu, ověřování a autorizaci koncových uživatelů představuje klíčovou funkci pro zajištění ověřování uživatelů, přidělování síťových prostředků uživatelům a správu uživatelskou relací za účelem dostupnosti služeb a zachování důvěrnosti komunikace v síti.

Vzhledem k tomu, že do množiny prvků představujících tuto nepominutelnou funkci se rovněž řadí zmíněné ověřování koncových zařízení uživatelů, kontrola a správa přístupů, včetně přidělování síťových prostředků skrz přiřazování IP adres koncovým zařízením a serverů sloužícím uživatelům, z hlediska dostupnosti je tato funkce klíčová.

Skrz přidělování síťových zdrojů musí uvedená funkce komunikovat s řadou dalších síťových funkcí, včetně funkcí nepominutelných, s čímž se pojí také riziko úniku dat v případě kompromitace dané funkce. V neposlední řadě se funkce také významně podílí na řízení síťového provozu, údržbě spojení a zajišťování dostupnosti služeb, důvěrnosti komunikací a informační bezpečnosti komunikační sítě jako celku.

Ad číslo 1.2

Další funkce, tj. registrace, autentizace a autorizace funkcí veřejné komunikační sítě a síťových služeb, patří mezi nepominutelné funkce vzhledem k síťovým registrům užívaným k uchovávání informací

o síťových funkcích, jež odpovídají za autorizaci jiných funkcí sloužících mimo jiné k řízení autorizace nebo účtování zpoplatněných služeb.

Primární účel funkcí čísla 1.2 je kontrola a řízení přístupu síťových funkcí k síti, činí z prvků výše uvedených nepominutelnou funkci podílející se na správě přístupu, zajišťování spojení a dostupnosti služeb, včetně napomáhání s důvěrností komunikace a informační bezpečností.

Ad číslo 1.3

Jak je uvedené v příloze, daná funkce umožňuje přístup k údajům o zeměpisné poloze koncových zařízení zpracovávaných v rámci veřejné komunikační sítě nebo určení polohy zařízení pomocí prostředků veřejné komunikační sítě, čímž odhaluje polohu koncového zařízení, zejména těch s předplacenými službami, tedy i zeměpisnou polohu uživatele za pomoci přijímání geoprostorových dat, včetně provozních a lokalizačních údajů důležitých pro přenos komunikace. Tyto údaje primárně slouží k řízení přístupu k síti, což z funkcí čísla 1.3 činí nepominutelnou funkci co do zajištění přístupu k síti, zejména významného pro případ nouzových situací, kdy je lokalizace uživatelů a zajištění jejich přístupu k síti zcela zásadní.

Ad číslo 1.4

Jedná se o funkce, které slouží převážně k ukládání a načítání síťových, zejména nestrukturovaných dat a dat koncových uživatelů. Ztráta nebo nemožnost načíst tato data má významný dopad na řízení a správu síťového provozu, převážně pro zajištění dostupnosti služeb uživatelů a zajištění důvěrnosti komunikace a informační bezpečnosti.

Ad číslo 1.5

Uvedené služby představují množinu síťových prvků, služeb a funkcí infrastruktury, které jsou nezbytné pro podporu provozu veřejné komunikační sítě a veřejně dostupné služby elektronických komunikací. Mezi tyto služby se řadí datová úložiště obsahující informace o nepominutelných funkcích veřejné komunikační sítě a údaje o uživatelích, služby přidělování adres a jmen v jádru sítě, tzv. časové služby sloužící pro synchronizaci času napříč funkcemi (významné pro správu klíčů a protokolů) a centralizovaný systém časových služeb.

Tyto služby jsou zásadní pro zajištění síťového provozu a v důsledky i pro dostupnost síťových služeb. Jejich role je zásadní pro správu přístupů různých síťových funkcí do veřejné komunikační sítě a synchronizaci síťového provozu, včetně zajištění důvěrnosti komunikace a informační bezpečnosti sítě jako celku.

Ad číslo 1.6

Zavádění rozhraní pro propojování jednotlivých sítí veřejných komunikací nebo služeb, jako je roaming, se týká zejména vnějších rozhraní jádra sítě, zajišťujících přístup k síťovým službám jiných veřejných komunikačních sítí poskytovaných jedním nebo více operátory. Zde se řadí jak roamingové služby umožňující propojování mezi sítěmi, tak rovněž internetové služby a jejich přístupové brány. Uvedené funkcionality jsou významné pro řízení a správu síťového provozu a přístupu k službám v síti, kvůli čemuž se funkce považuje za důležitou pro zajištění dostupnosti služeb a informační bezpečnost.

Ad číslo 1.7

Množina funkcí upravená číslem 1.7 zahrnuje funkce zpřístupňující jádro sítě třetím stranám, zejména jiným veřejným komunikačním sítím z hlediska bezpečnosti a přístupu k nim. Funkce je oproti obecnému pojetí považována za nepominutelnou, jelikož slouží jako praktický překladač programových funkcí. Jedná se o přístupovou bránu do jádra sítě, což ji činí zásadní pro zajištění bezpečnost jádra veřejné komunikační sítě.

Ad číslo 1.8

Tato funkce zahrnuje propojovací body zajišťující spojení s jinými veřejnými komunikačními sítěmi a službami umožňujícími přenos provozu mezi uvedenými sítěmi, a to včetně internetového přenosu.

Z praktického hlediska tato skupina funkcí zahrnuje mimo jiné internetové výměnné body (IXP) a propojovací body mezi mobilními operátory, které slouží k výměně síťového provozu, například hlasových služeb, SMS nebo mobilních dat, mezi jednotlivými mobilními sítěmi.

Tyto funkce se používají k řízení a správě síťového provozu a vzhledem ke své klíčové roli při zajišťování provozuschopnosti sítí, dostupnosti služeb a informační bezpečnosti je třeba je považovat za kritické části komunikační infrastruktury

Ad číslo 1.9

Uvedené funkce zahrnují centralizované funkce sloužící k ukládání, přenosu, zajištění integrity a řízení šifrovacích klíčů uživatelů. V uvedeném případě centralizovanost funkce spočívá v jednotném účelu funkce, což představuje situaci, kdy může být daná funkce rozdělena do několika různých komponent v různých zeměpisných lokacích.

Primární účel funkce čísla 1.9 se vztahuje zejména na oblasti šifrování síťového provozu mezi základnovými stanicemi sítě a jádrem sítě, a to včetně bezdrátových přenosových spojů základnových stanic, šifrování používané komponentami jádra sítě a šifrování funkcí páteřní veřejné komunikační sítě. Zahrnuje rovněž šifrování datových úložišť používaných kritickými částmi komunikační sítě. Dále se písmeno vztahuje nejen na ověřování a šifrování mezi uživateli a sítí, ale také na ověřování a šifrování mezi jednotlivými síťovými prvky a síťovými funkcemi.

Kritickou součástí uvedených funkcí je řízení a správa síťového provozu a přístupu uživatelů k síti, jelikož je významná při zajišťování důvěrnosti komunikace a informační bezpečnosti komunikační sítě jako celku

Ad číslo 1.10

Dané číslo zahrnuje funkce užívané k monitorování, správě nebo filtrování síťového provozu nebo ke zpracování dat protokolů systémů připojených k dalším nepominutelným funkcím veřejné komunikační sítě. Množina čísla 1.10 se rovněž vztahuje na funkce používané ke správě a monitorování opatření týkajících se údržby nebo správy sítě.

Hlavním smyslem zabezpečení informací je ochrana jádra sítě jak před hrozbami zvnějšku, tzn. ze strany externích veřejných komunikačních sítí, tak rovněž zevnitř ze strany ostatních funkcí sítě. Dále podpora informační bezpečnosti, jako je bezpečnostní software na serverech, umožňuje správu platforem kritických systémů nebo jejich operačních systémů. Odstavec zahrnuje také funkce informační bezpečnosti zaměřené na další kritické části komunikační sítě, jako jsou například ty, jež řídí spojení. Pro zajištění své funkčnosti může být funkce čísla 1.10 z hlediska architektury sítě implementována i mimo jádro veřejné komunikační sítě, tj. na okrajové síti.

Ad číslo 1.11

Systémy řízení a monitorování veřejné komunikační sítě zpravidla mají významný dopad na přístup k síti a řízení provozu v dané síti. Uvedené systémy řízení a monitorování se vztahují na software a jiná zařízení, která se používají k provozu, údržbě a monitorování zdrojů komunikační sítě, včetně systémů zabezpečení informací, síťových zařízení či obecně softwaru používaného pro síťovou údržbu.

Významný dopad uvedených funkcí spočívá ve skutečnosti, že jsou dané funkce čísla 1.11 schopny umožnit či znemožnit přístup uživatelů nebo jiných nepominutelných funkcí k síti nebo službám sítě.

Ad číslo 1.12

Tato funkce zahrnuje systémy, jejichž správná funkce je nezbytná pro poskytování služeb veřejné komunikační sítě. Jejich výpadek může přímo ohrozit dostupnost nebo správu služeb, a proto jsou považovány za kritické.

Fakturační systémy (invoicing systems) zajišťují mimo jiné ověřování oprávnění k přístupu u předplacených služeb. V případě jejich nefunkčnosti může být znemožněn přístup uživatelů k síti nebo k některým jejím funkcím. Tyto systémy jsou často přímo napojeny na síťové prvky a další kritické systémy.

Podpůrné a back-end systémy, například tzv. Business Support Systems (BSS), jsou klíčové pro správu zákaznických dat, objednávek, aktivace služeb nebo řízení přístupu. Pokud jsou využívány v reálném čase a mají přímý vliv na poskytování služeb, je nutné je považovat za nepominutelnou (kritickou) funkci. Tyto systémy mohou být integrovány jak v rámci jádra sítě, tak mimo něj.

Ad číslo 1.13

Funkce zavádějící záznam a monitorování provozních a lokalizačních údajů slouží zejména k zajištění bezproblémového síťového provozu a přístupu k síti. Jejich smyslem je monitorování možných hrozeb a škodlivých událostí v souvislosti s přístupem uživatelů k síti v případě lokalizačních údajů a provozem sítě v případě monitorování provozních údajů. Tyto funkce jsou nezbytné pro zajištění přístupu a informační bezpečnosti veřejné komunikační sítě. Jejich podstata je totiž monitorovat, identifikovat a zaznamenávat škodlivé údaje.

Ad číslo 1.14

Systémy řízení základnových stanic spravující přístup uživatelů k veřejné komunikační síti se již kvůli schopnosti spravovat přístup uživatelů považují za nepominutelné funkce ve smyslu návrhu nařízení. V této souvislosti se funkce řízení rádiové přístupové sítě a řízení základnových stanic vztahuje na software a zařízení, která se používají k provozu, údržbě či správě a monitorování základnových stanic 2. generace sítí, tj. veřejných komunikačních sítí využívajících digitálního přenosu rádiového signálu ve standardu GSM, a dále také 4. a 5. generace sítí. Přístup k základnovým stanicím má zcela zásadní vliv na přístup uživatelů k veřejné komunikační síti.

Ad číslo 1.15

Virtualizace sítě je obecně považována za kritickou součást systémů elektronických komunikací, neboť mezi virtualizovanými funkcemi dochází ke sdílení zdrojů, což může z hlediska bezpečnosti informací představovat významné riziko. To je dáno vzájemnou závislostí virtualizovaných funkcí, které se v síti elektronických komunikací neustále ovlivňují například skrz sdílení zdrojů. Přístup k platformě virtualizované funkce má potenciál ohrozit ostatní funkce, z čehož vyplývá, že síťové funkce, které jsou virtualizované na stejné platformě jako jádro sítě, spadají pod tuto nepominutelnou funkci virtualizace sítě. Pokud je tak například centrální jednotka (CU) virtualizovaná na stejné platformě jako jádro sítě, bude i tato spadat pod nepominutelné funkce čísla 1.15.

Ad 2. Nepominutelné funkce sítí 4. generace - veřejná komunikační síť provozovaná s využitím standardu 3GPP LTE (Release 8 a vyšší) nebo standardem IEEE 802.16m

Tato část přílohy definuje funkce sítě, které jsou považovány za nepominutelné funkce mobilní veřejné komunikační sítě 4. generace, tedy tzv. 4G mobilní sítě, s odkazem na síťové funkce, které jsou popsány technickými specifikacemi TS 23.002 organizace 3GPP. Ne všechny funkce, na něž zmíněné technické specifikace odkazují, především v rámci bodů 4.1.1, 4.1.4 nebo 4.1.5 těchto specifikací, mohou být považovány za nepominutelné. Z toho důvodu jsou v tabulce přílohy umístěny pouze takové funkce,

které jsou technickými specifikacemi považovány za kritické části komunikační sítě tak, jak je chápe 3GPP.

Seznam nepominutelných funkcí pro 4. generaci sítí, tak jak je uveden v tabulce přílohy, není taxativní, a správce sítě nebo povinná osoba má posoudit, zda v jejich síti existují kromě funkcí uvedených v tabulce i další kritické funkce, které lze určit spojením funkcí 4. nebo 5. generace sítí s definicí veškerých funkcí veřejné komunikační sítě, jak je uvedeno v první části přílohy.

Funkce 4. generace sítí uvedené v příloze obsahují logický výčet, kdy by každá uvedená funkce měla být považována za nepominutelnou funkci podle technických specifikací 3GPP i v případě, kdy komponenta implementují jen část uvedené funkce, nikoliv celý rozsah funkce, která je přílohou určena jako nepominutelná. Zároveň platí, že softwarové komponenty mohou podporovat více než jednu funkci uvedenou v tabulce.

Nutno dodat, že kromě technologií LTE, určené konkrétně 3GPP LTE (Release 8 a vyšší) nebo IEEE 802.16m, či LTE Advanced, se uvedený seznam nepominutelných funkcí pro

4. generaci vztahuje i na tzv. režim 5G NSA, tedy tzv. non stand-alone mód 5. generace sítí. Tento režim označuje situaci, kdy funkce sítě 5. generace pracují na infrastruktuře sítě 4. generace. Seznam funkcí v příloze je také ve shodě s analogickými seznamy kritických funkcí sítí elektronické komunikace ve Spojeném království, Francii a Finsku, které jsou blíže představeny v obecné části této důvodové zprávy.

Ad číslo 2.1

První funkce seznamu představuje centrální databázi, která obsahuje údaje pro zpracování uživatelských relací a jejich připojení k síti elektronické komunikace založené na technologii LTE. Tato funkce převážně zpracovává správu přístupu uživatelů, jejich identifikaci, profilaci a mobilitu. Mimo to je funkce odpovědná za správu klíčů a vytváření ochranných vektorů pro ověřování uživatelů, s čímž souvisí i její další funkcionalita, kterou je provádění tzv. odposlechu a sledování komunikace skrz tzv. Lawful Interception (dále také „LI“). Podle technických specifikací funkce č. 2.1 zahrnuje další funkce, jako je tzv. Home Location Register nebo Authentication Centre.

Zmíněné ukládání dat pro zpracování uživatelských relací slouží i ke kontrole a správě přístupu uživatelů k síti, což souvisí s řízením sítě elektronických komunikací, konkrétně s řízením provozu uvnitř této sítě, údržbou spojení a zajišťováním dostupnosti komunikačních služeb. Tato funkce významně ovlivňuje důvěrnost síťové komunikace a informační bezpečnost sítě elektronických komunikací, pročež musí být tato funkce považována za nepominutelnou.

Ad číslo 2.2

Uvedená funkce Packet Gateway (PGW) představuje tzv. síťovou bránu pro paketová data, to znamená, že PGW funguje jako rozhraní mezi sítí LTE a dalšími sítěmi, přičemž pracuje s tzv. paketovými daty, užívanými ve službách typu internet nebo sítě IMS založené na protokolu SIP. Tato funkce zahrnuje další služby, zejména správu kvality služeb, tzv. Quality of Service, zkráceně QoS, či hloubkovou kontrolu paketů.

Funkce je považována za nepominutelnou vzhledem k její klíčové roli pro integraci velkého množství funkcí jádrové sítě, zajištění dostupnosti dat či možnosti detekce, blokování nebo zachycení síťového provozu.

Ad číslo 2.3

Tato brána přepojující pakety mezi vnitřní IP sítí operátora a externí IP sítí je funkcí, jež také zaštiťuje přidělování IP adres koncovým zařízením, vynucování zásad používání sítě nebo filtrování a analýzu provozu, což souvisí s umožněním účtovat úhrady a řídit provoz sítě elektronických komunikací.

Vzhledem k tomu, že se funkce Packet Data Network Gateway (PDN-GW) čísla 2.3 považuje za součást řízení a správy síťového provozu, je tato funkce taktéž považována za kritickou, a tedy nepominutelnou součást sítě elektronických komunikací. Uvedená funkce má zásadní roli při zajišťování dostupnosti služeb a důvěrnosti komunikace v síti.

Ad číslo 2.4

Daná funkce Evolved Packet Data Gateway (ePDG) jednak vytváří přístup k jinému nežli 3GPP směrování provozu, zejména mezi funkcí PDN-GW a uživatelem, jednak implementuje služby VoWiFi, tedy služby bezdrátového volání přes tzv. místní síť Voice over Wi-Fi. Funkce ePDG také aktivuje výměnu klíčů mezi uživatelem k vytvoření bezpečného komunikačního tunelu, včetně ověřování a autorizace v rámci tohoto tunelu s implementací funkce LI.

Jelikož tato funkce řídí a spravuje síťový provoz, je považována za kritickou, tedy nepominutelnou funkcí sítě elektronických komunikací. Funkce zajišťuje dostupnost služeb, převážně skrz udržování spojení mezi uživateli, a důvěrnost komunikace v síti.

Ad číslo 2.5

Uvedená funkce Policy and Charging Rules Function (PCRF) zajišťuje, aby provoz v síti na uživatelské úrovni odpovídal profilům jednotlivých uživatelů ve veřejné komunikační síti. Funkce svou povahou zajišťuje kvalitu služeb připojení uživatelů a implementuje zpoplatnění hlasových služeb VoLTE nebo tzv. roamingu. Jelikož funkce slouží k řízení a správě síťového provozu, primárně pak k přístupu uživatelů k síti, je tato považována za nepominutelnou pro potřeby veřejných komunikačních sítí. PCRF významně napomáhá k zajišťování dostupnosti služeb v podobě údržby a řízení spojení.

Ad číslo 2.6

Tato funkce zajišťuje správu připojení koncových zařízení k mobilní síti na úrovni řídicí roviny. Mobile Management Entity (MME) je odpovědná za registraci zařízení, řízení mobility, autentizaci uživatelů a směrování signalizačního provozu a hraje tak klíčovou roli při zajištění roamingových služeb a kontinuity spojení v rámci sítě.

Vzhledem ke své úloze při řízení přístupu k síti a zajištění jejího provozu je tato funkce považována za nepominutelnou. Je zásadní pro dostupnost služeb, správu síťového provozu a zajištění důvěrnosti a bezpečnosti komunikace v mobilních sítích.

Ad číslo 2.7

Serving Gateway (SGW) je síťová funkce zajišťující přenos datového provozu mezi základnovými stanicemi (eNodeB) a bránou do vnějších sítí (PDN-GW). Tato funkce se nachází na tzv. uživatelské rovině (user plane) a zajišťuje směrování a přeposílání uživatelského provozu, a to jak při běžné komunikaci, tak při mobilitě uživatelů (např. při předávání mezi základnovými stanicemi – handover).

Vzhledem k tomu, že bez funkce SGW není možné zajistit přenos dat mezi koncovým zařízením a sítí, jedná se o nepominutelnou funkci, která má zásadní význam pro dostupnost služeb veřejné komunikační sítě.

Ad číslo 2.8

Funkce Subscription Locator Function (SLF) předává název centrální databáze dalším nepominutelným funkcím, jako je AAA. Uvedené slouží k řízení a správě přístupů uživatelů k síťovým službám, což staví funkci SLF do role nepominutelné funkce z hlediska kontroly, řízení sítě elektronických komunikací a jejího provozu, dostupnosti spojení a služeb, důvěrnosti komunikace a bezpečnosti informací.

Ad číslo 2.9

Registr identit Equipment Identity Register (EIR) představuje databázi veřejné komunikační sítě sloužící primárně k registru totožnosti jednotlivých zařízení. EIR zejména uchovává mezinárodní identifikační čísla mobilních zařízení a informuje ohledně oprávnění užívat jednotlivá mobilní zařízení v síti. EIR zároveň spravuje tzv. černou listinu, která znemožňuje přístup všech koncových zařízení a adres uvedených na listině k síti elektronických komunikací.

Z výše uvedeného vyplývá funkcionalita EIR jakožto kontrolora přístupu uživatelů k síti, což řadí EIR mezi nepominutelné funkce sítě elektronických komunikací. Funkce také slouží k zabránění používání neoprávněných zařízení v síti, k zajištění dostupnosti síťových služeb a informační bezpečnosti.

Ad číslo 2.10

3GPP AAA Server kromě zajištění autorizace také spravuje mobilitu uživatelů s přístupem mimo 3GPP a ukládá údaje o uživatelích za účelem správy přístupu, jenž jsou potřebné převážně ke správě přístupu do sítě. Další funkcionalitou 3GPP AAA serveru je také implementace služby VoWiFi a funkce LI. Z důvodu řízení přístupu uživatelů k síti se považuje tato funkce za nepominutelnou funkci sítě elektronických komunikací. Představuje významnou roli pro zajištění důvěrnosti komunikace, kontrolu, správu, provoz, a tím pádem i dostupnost sítě jako celku.

Ad číslo 2.11

Proxy server odpovědný za ověřování a autorizaci uživatelů s přístupem mimo 3GPP oproti předchozímu 3GPP AAA serveru poskytuje odpovídající služby jako 3GPP AAA, ale pro služby roamingu. Dále zmíněný Proxy AAA server vybírá bránu pro relace uživatele pro roaming. Z toho vyplývá významná role uvedené funkce pro zajištění přístupu uživatelů k síti, která určuje Proxy AAA Server jako nepominutelnou funkci sítě elektronických komunikací.

Ad číslo 2.12

Funkce řídící uživatelský provoz mezi mobilní sítí a přístupovými sítěmi mimo 3GPP se týká sítí jako je WLAN a sdílí data za účelem směrování provozu a mobility koncových zařízení v síti, což slouží k řízení a správě síťového provozu uživatelů. Funkce také významně přispívá k zajištění dostupnosti sítě a služeb, a je tudíž považována ze nepominutelnou pro sítě elektronických komunikací.

Ad 3. Nepominutelné funkce sítí 5. generace - veřejná komunikační síť vyhovující standardu sítí elektronických komunikací podle specifikace 3GPP/ETSI zahrnující minimálně standard přístupové rádiové sítě 5G NR (New Radio) v architektuře, která splňuje požadavky specifikací ETSI TS 123 501 (3GPP TS 23.501) a ETSI TS 138 401 (3GPP TS 38.401) nebo aktuálnějších.

V pořadí třetí část přílohy určuje funkce 5. generace mobilní veřejné komunikační sítě, jež lze považovat za nepominutelné z hlediska jejich kritičnosti popsané převážně v technických specifikacích 3GPP TS 23.501. Funkce určené ve zmíněných specifikacích jsou standardizované, dobře popsané a často rozdělené mezi vícero aplikací nebo komponent. Výčet extrahovaných kritických funkcí pro 5. generaci sítí je uveden v tabulce přílohy.

Každá funkce z této části přílohy by měla být považována za nepominutelnou funkci také v případě, kdy jednotlivá komponenta podporují pouze část uvedené funkce, která je určená jako nepominutelná.

Pro potřeby návrhu nařízení je 5. generace sítí chápána jako veřejná komunikační síť vyhovující standardu sítí elektronických komunikací podle specifikace 3GPP/ETSI, zahrnující minimálně standard přístupové rádiové sítě 5G NR (New Radio) v architektuře, která splňuje požadavky specifikací ETSI TS 123 501 (3GPP TS 23.501) a ETSI TS 138 401 (3GPP TS 38.401) nebo aktuálnějších.

Ad číslo 3.1

Funkce Authentication Server Function (AUSF) spravuje funkce spojené s ověřováním koncových zařízení uživatelů a zároveň poskytuje jednotný rámec pro ověřování připojení. Primární funkcionalitou AUSF je správa síťového provozu a přístup uživatelů k síti, kvůli čemuž je funkce považována za nepominutelnou. Její další role je uplatňována při zajišťování dostupnosti sítě, služeb, zaručení důvěrnosti komunikace a informační bezpečnosti sítí elektronické komunikace.

Ad číslo 3.2

Funkce Access and Mobility Management Function (AMF) kromě účelu popsaném v příloze slouží k připojení základnových stanic a koncových zařízení rádiové sítě a jejich registrace k jádru sítě, jakož i samotné správě mobility. Dále AMF vytváří, spravuje a obstarává přesah přístupu koncových uživatelů k sítím mimo mobilní síť, jako např. k WLAN. K AMF se rovněž váže možnost tzv. odposlechu síťového provozu a sledování komunikace skrz funkci LI.

Role AMF při kontrole a správě přístupu uživatelů k síti znamená určení AMF jako nepominutelné funkce, která má významnou roli pro řízení síťového provozu, udržování spojení, zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnost sítě elektronických komunikací jako celku.

Ad číslo 3.3

Funkce Unstructured Data Storage Function (UDSF), bývá zpravidla využívána ostatními funkcemi k ukládání a načítání nestrukturovaných dat, která se vážou k údajům ohledně připojení, stavu jednotlivých funkcí, včetně těch nepominutelných, či obecně relacím v síti. V případě jejího využití funkce UDSF přispívá k řízení a správě síťového provozu, čímž musí být považována za nepominutelnou funkci sítě elektronických komunikací. Účel její implementace přispívá k zajištění dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti sítě elektronických komunikací.

Ad číslo 3.4

Funkce Network Exposure Function (NEF) umožňující poskytování funkcí jádra 5G sítě třetím stranám a externím aplikacím mimo jiné umožňuje i bezpečnou komunikaci jiných funkcí se sítí a ukládání dat těchto funkcí. Jako nepominutelná je tato funkce považována z důvodu řízení přístupu uživatelů k funkcím sítě, což je klíčové pro důvěrnost komunikace, přístupu k službám a informační bezpečnost sítě.

Ad číslo 3.5

Daná funkce Intermediate Network Exposure Function (I-NEF), umožňující poskytování funkcí jádra 5. generace sítě třetím stranám a externím aplikacím, funguje téměř totožně jako funkce NEF s tím rozdílem, že je tato funkce užívána pro roaming. Z toho důvodu je považována za nepominutelnou.

Ad číslo 3.6

Funkce Network Repository Function (NRF) spravuje seznam síťových služeb a komponent, čímž obstarává registraci služeb a vyhledávání funkcí. Usnadňuje tak vzájemnou dostupnost či komunikaci jednotlivých funkcí a služeb v síti. Jelikož všechny funkce sítě 5. generace komunikují s NRF, její význam je naprosto stěžejní pro předávání informací, čímž se řadí do seznamu nepominutelných funkcí. Její role je zásadní pro dostupnost sítě a služeb a informační bezpečnost sítě.

Ad číslo 3.7

Funkce Network Slice Selection Function (NSSF) slouží mimo jiné ke kontrole a výběru povolených nebo obecně koncových zařízení sítě. Funkce spravuje síťový provoz a přístup uživatelů k síti, což z ní

dělá nepominutelnou funkci pro zajištění dostupnosti sítí, služeb, důvěrnosti komunikace a informační bezpečnost sítě.

Ad číslo 3.8

Funkce Network Slice Specific Authentication and Authorisation Function (NSSAAF) slouží ke kontrole a správě přístupů uživatelů k síti elektronických komunikací, což je významné pro zajištění dostupnosti služeb, důvěrnosti komunikace a dat a informační bezpečnosti sítě. Uvedené NSSAAF řadí mezi nepominutelné funkce.

Ad číslo 3.9

Tato funkce Policy Control Function (PCF) je odpovědná za řízení provozu a zavedení politiky přístupu, tedy zásad řízení přístupu, kdy zmíněná funkce představuje zásadní prvek pro řízení kvality služeb a zpoplatňování služeb v síti elektronických komunikací. PCF tak určuje politiky podporující rozdělení sítě, politiky mobility a roamingu. Uvedené skutečnosti z ní činí jednotku podílející se na řízení i správě síťového provozu a přístupů uživatelů k síti a řadí ji tak mezi nepominutelné funkce veřejné komunikační sítě, kdy je PCF obzvlášť významná pro zajištění dostupnosti služeb sítě.

Ad číslo 3.10

Funkce řídící uživatelské relace, Session Management Function (SMF), kombinuje a spravuje více funkcí řízení provozu správy relací podle síťových protokolů, přiděluje IP adresy a rovněž implementuje funkci LI. Její role je významná v řízení a správě síťového provozu. Ze zmíněného a z důvodu zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti veřejné komunikační sítě, se funkce řadí mezi nepominutelné funkce.

Ad číslo 3.11

Funkce Unified Data Management (UDM) mimo funkcionality zmíněné v příloze odpovídá za identifikaci a registr uživatelů, správu předplatného a vytváření a správy šifrovacích klíčů. UDM dále definuje nebo odstraňuje účastníky ve veřejné komunikační síti 5. generace, monitoruje výměnu karet SIM, změnu čísel MSISDN nebo upravuje údaje o objednávkách. Protože funkce vykonává další práci obdobnou funkci HSS a implementuje funkci LI, její role při řízení a kontrole uživatelů k síťovým službám ji činí nepominutelnou.

Ad číslo 3.12

Datové úložiště Unified Data Repository (UDR) představuje významnou funkci pro ukládání a načítání dat, včetně strukturálních a aplikačních dat z nepominutelné funkce NEF. Úlohou UDR je řídit a spravovat síťový provoz a zajistit tak dostupnost služeb, důvěrnost komunikace a informační bezpečnost sítě. To z UDR činí nepominutelnou funkci sítí elektronických komunikací.

Ad číslo 3.13

Funkce User Plane Function (UPF) je primárně odpovědná za řízení kvality služeb, filtrování a šifrování provozu na uživatelské rovině nebo udržování kontinuity relací a síťových služeb. Funkce tedy slouží k řízení a správě síťového provozu uživatelů, a tudíž se řadí mezi nepominutelné funkce obstarávající dostupnost spojení a důvěrnost komunikace.

Ad číslo 3.14

Funkce pro ukládání a uchovávání identifikačních dat uživatelských zařízení mimo zmíněné ukládá údaje o rádiových schopnostech koncových zařízení, což zahrnuje informace

o podporovaných rádiových technologiích či kmitočtových pásmech, jakož další schopnosti rádiové sítě. Ze své podstaty funkce zajišťuje kontrolu a řídí přístup k sítí, což z ní činí nepominutelnou funkci podílející se na zajištění dostupnosti služeb.

Ad číslo 3.15

Funkce Application Function (AF) především určuje směrování na základě aplikací uživatelů a skrz nepominutelnou funkci NEF také komunikaci s jádrem sítě. Primárně má tato funkce za cíl řídit a spravovat síťový provoz, konkrétně přístup k síti natolik významným způsobem, že je tato funkce považována za nepominutelnou co do zajištění dostupnosti služeb a z toho vyplývající informační bezpečnosti sítě.

Ad číslo 3.16

Registr identit zařízení a vybavení 5G-Equipment Identity Register (5G-EIR) vytváří tzv. černou listinu, jež znemožňuje přístup nepovoleným zařízením k veřejné komunikační síti. Účel funkce, spočívající v kontrole a řízení přístupu uživatelů do sítě na základě uvedené černé listiny, řadí 5G-EIR mezi nepominutelné funkce. Této funkce lze přisuzovat zásadní roli v zajištění dostupnosti služeb z důvodu řízení přístupu.

Ad číslo 3.17

Funkce Network Data Analytics Function (NWDAF) shromažďující a analyzující data pro řízení sítě využívá strojové učení, tzv. machine learning, ke shromažďování dat a poskytování těchto dat ostatním funkcím v reálném čase. K dalším, neméně podstatným funkcionalitám NWDAF se řadí provádění prediktivních analýz a proaktivní správa 5. generace sítí. NWDAF představuje komplexní funkci, která rovněž slouží k automatizovanému škálování síťové infrastruktury, přiřazování síťových úseků, správě přístupů do těchto úseků a zajištění mobility v síti.

Vzhledem k rozšíření NWDAF musí být naplněna složka podstatného řízení provozu v síti. To znamená, že v případě distribuované implementace s jednou nebo nižšími jednotkami NWDAF je tato funkce považována za nepominutelnou vždy, jelikož v těchto případech významně řídí a spravuje síťový provoz. NWDAF představuje obzvlášť významný nástroj pro dostupnost služeb.

Ad číslo 3.18

Funkce umožňující online a offline platby Charging Function (CHF) představuje funkci významnou pro způsoby účtování za služby poskytované v rámci využívání sítě elektronických komunikací. Funkce CHF komunikuje s ostatními funkcemi 5. generace sítí a podporuje zpracování informací o účtování uživatelů, dále také generuje tzv. tikety, tedy systémové požadavky vyřešit problém, směruje síťový tok zpráv o účtování a monitoruje poruchy nebo výpadky související s účtováním. Význam funkce tkví v monitorovacích schopnostech funkce a zajištění důvěrnosti komunikace mezi funkcemi, což z CHF činí nepominutelnou funkci.

Ad číslo 3.19

Funkce směrování zpráv do ostatních síťových funkcí Service Communication Proxy (SCP) kromě směrování a přenášení zpráv mezi funkcemi zjednodušuje topologii veřejné komunikační sítě, vyrovnává zátěž sítě nebo možné přetížení co do množství zpráv za účelem integrace v prostředí s větším množstvím komponent. Z tohoto důvodu je funkce považována za nepominutelnou, pakliže skrz řízení přenášení zpráv obstarává významnou roli při zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti.

Ad číslo 3.20

Proxy server Security Edge Protection Proxy (SEPP) podporuje skrytí topologie sítě a zavádí filtrování zpráv, včetně jejich monitorování, na rozhraní řídící i uživatelské roviny mezi mobilními sítěmi. To ve své podstatě znamená také zajištění přístupu do jiných sítí v případě užívání služeb roamingu a obecně podílení se na řízení a správě síťového provozu, pročež je funkce považována za nepominutelnou.

Ad číslo 3.21

Funkce Non-3GPP InterWorking Function (N3IWF) kromě uvedeného v příloze také umožňuje přístup k jádru 5. generace veřejné komunikační sítě prostřednictvím bezdrátové místní sítě WLAN. Tato funkce také podporuje vytvoření zabezpečeného komunikačního tunelu s koncovými zařízeními a autorizuje přístup uživatelů k jádru sítě 5G. Jelikož tímto zajišťuje dostupnost služeb, obstarává důvěrnost komunikace a v důsledku také informační bezpečnost celé sítě, tak je její role nepominutelná.

Ad číslo 3.22

Funkce Trusted Non-3GPP Gateway Function (TNGF) představuje součást přístupové sítě tzv. Trusted Non-3GPP Access Network. Její účel spočívá v zajištění postupného propojení uživatele s jádrem sítě. V praktickém užití je funkce TNGF analogií N3IWF, ovšem vyjma možnosti použití šifrovaného tunelu. Z toho důvodu se, tak jako N3IWF, řadí mezi nepominutelné funkce sítě elektronické komunikace.

Ad číslo 3.23

Funkce propojení Wireline Access Gateway Function (W-AGF) zajišťuje zpřístupnění sítě 5. generace sítí koncovým zařízením uživatelů. Význam funkce spočívá také v konvergenci bezdrátového a drátového připojení s jednotným zajištěním bezpečnostně přístupových postupů, jakož i zajištění kvality služeb nebo podpory řízení provozu. Funkce je tak zařazena na seznam nepominutelných funkcí.