AKOS
AGENCIJA ZA KOMUNIKACIJSKA OMREŽJA IN STORITVE REPUBLIKE SLOVENIJE

Številka: 0073-3-2023/70
Datum: 10. 10. 2023

ZADEVA: Odgovori na pripombe zainteresirane javnosti glede predloga Splošnega akta o dodatnih varnostnih zahtevah in omejitvah

Agencija za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju: agencija) obvešča javnost, da je na podlagi šestega odstavka 116. člena Zakona o elektronskih komunikacijah - ZEKom-2 (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) pripravila predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (v nadaljevanju: SA ali splošni akt)

Prvi predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah je agencija objavila na svoji spletni strani dne 6. 4. 2023 ter pozvala zainteresirano javnost, naj poda pripombe, predloge in dopolnitve.

Agencija je v okviru predmetnega (istega) postopka sprejemanja SA nato pripravila nov predlog in ga dala v daljše (zaradi katastrofalnih poplav v Republiki Sloveniji) javno posvetovanje. Veliko pripomb, prejetih v prvem delu posvetovanja ni bilo več relevantnih. V spodnjih odgovorih je agencija poskusila povzeti vse relevantne pripombe, ki se nanašajo na predlog splošnega akta katerega javno posvetovanje se je zaključilo 18. septembra 2023.

Do izteka roka je agencija prejela pripombe naslednjih deležnikov:

- **Gospodarska zbornica Slovenije, Združenje za informatiko in telekomunikacije Gospodarske zbornice Slovenije,** Dimičeva 13, 1504 Ljubljana (v nadaljevanju: GZS),
- **Telemach Slovenija d.o.o.,** Brnčičeva ulica 49A, Ljubljana, 1231 Ljubljana-Črnuče (v nadaljevanju: Telemach) ,
- **Telekom Slovenije, d.d.,** Cigaletova ulica 15, 1000 Ljubljana (v nadaljevanju: Telekom Slovenije),
- **T - 2 d.o.o.**, Verovškova ulica 64A, Ljubljana, 1000 Ljubljana (v nadaljevanju: T2),
- **Huawei** Technologies Ljubljana d.o.o., Ameriška ulica 8, Ljubljana, 1000 Ljubljana (v nadaljevanju: Huawei).

Agencija je prejeta mnenja in pripombe na zadnjo različico Splošnega akta, dne 25. 9. 2023 objavila na svoji spletni strani.

V nadaljevanju agencija povzema prejete pripombe, predloge in mnenja po posameznih deležnikih ter se opredeljuje do njih. Do vključno 18. 9. 2023 so prispeli predlogi in mnenja:

I. Pripombe, predlogi in mnenja GZS z dne, 21. 8. 2023 in 18. 9. 2023 ter odgovori AKOS

GZS (pripombe in mnenja GZS z dne 21. 8. 2023) zanima kateri so pomembni dogodki, ki naj bi se zgodili na nacionalnem in na evropskem nivoju, ki naj bi vplivali na vsebino in zahteve predmetnega splošnega akta in spremembe na evropski in nacionalni ravni, v luči katerih naj bi bil pripravljen nov predlog splošnega akta?

Odgovor agencije:

Med ključnimi so ugotovitve poročila Skupine za sodelovanje glede varnosti omrežij in informacij (NIS Cooperation Group) o napredku držav članic, pri izvajanju Sklopa orodij EU za varnost 5G glede implementacije strateških ukrepov. Pri presoji kritičnosti posameznih elementov omrežja, je agencija izhajala tudi iz usklajenih ocen tveganj za omrežja 5G na ravni EU (Ocena tveganj). Med ključnimi ugotovitvami poročila Skupine za sodelovanje glede varnosti omrežij in informacij (NIS Cooperation Group) glede napredka držav članic pri izvajanju Sklopa orodij EU za varnost 5G (EU Toolbox for 5G security) glede implementacije strateški ukrepov, ki se nanašajo na dobavitelje z visokim tveganjem, je bilo med drugim izpostavljeno, da naj države članice pri oceni profila tveganja dobaviteljev, upoštevajo kriterije priporočene v Sklopu orodij EU za varnost 5G, saj je očitno, da so med dobavitelji 5G opreme očitne razlike v njihovih značilnostih, zlasti kar zadeva verjetnost vpliva nanje s strani določenih tretjih držav, katerih varnostna zakonodaja in korporativno upravljanje sta potencialno tveganje za varnost Unije. Poročilo državam jasno nalaga, da morajo za učinkovito zmanjšanje tveganj zagotoviti, da se posebne omejitve nanašajo tako na kritične kot tudi zelo občutljive elemente omrežja, opredeljene v Usklajeni oceni tveganj, vključno z radijskim dostopovnim omrežjem (RAN).

V mesecu juniju 2023 je prišlo tudi do novih ugotovitev, ki jih je Evropska komisija zapisala v svojem sporočilu[1], in sicer da so države članice, ki so omejile ali izključile iz omrežij 5G določena podjetja, v celoti skladne s Priporočilom, Sklop Orodij EU za varnost 5G omrežij, na kar se je skliceval v svojem govoru[2] v zvezi s stanjem kibernetske varnosti 5G omrežij na ravni EU tudi Evropski komisar za notranji trg Thierry Breton. Nove ugotovitve v zvezi s stanjem kibernetske varnosti 5G omrežij na ravni EU pa so zajete tudi v Drugem poročilu držav članic o napredku implementacije ukrepov iz 5G Toolbox-a[3]. Nenazadnje pa je bil s strani Vlade

[1] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3309
[2] https://ec.europa.eu/commission/presscorner/detail/en/speech_23_3314
[3] https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

Republike Slovenije sprejet tudi sklep št. 381000-2/2023/2 z dne 22.6.2023 in Priporočila URSIV.

GZS zanimajo kakšna so priporočila, ki jih je prejel AKOS od URSIV v zvezi z uvrstitvijo RAN med kritične elemente omrežja? Katera dejstva in ugotovitve izhajajo iz priporočila URSIV in so vplivala na predlog splošnega akta?

Odgovor agencije:

Agencija sodeluje z URSIV v obliki delovnih sestankov, kjer se razpravlja o vseh relevantnih virih za odločanje v tej zadevi in skladno z njimi oblikuje besedilo predloga splošnega akta.

URSIV je Agenciji, v zvezi s problematiko, dne 28. 7. 2023 poslal tudi dokument z naslovom: Priporočilo agenciji pri določanju kritičnih elementov omrežja št. 007-3/2023-1544-18, v katerem predstavi argumente in dokumentacijo za oblikovanje stališča Agencije do umestitve določenih kritičnih elementov v predmetni Splošni Akt.

Kljub temu je potrebno izpostaviti, da je agencija pri svojem delu samostojna (230 člen ZEKom-2) in se odloča na podlagi predstavljenih argumentov in stališč posameznih organov in zastopnikov drugih interesov pri čemer zasleduje zlasti javni interes kot je razviden iz veljavnih pravnih aktov.

GZS sprašuje ali je AKOS pri pripravi splošnega akta upošteval nacionalna in mednarodno uveljavljena spoznanja stroke glede razporeditve med kritične in nekritične dela omrežja, kakor izhajajo iz: nacionalne ocene tveganj RS glede informacijske varnosti 5G, Usklajene ocene tveganj, Nabora orodji za varnost omrežji 5G, standardov ETSI/3GPP, smernic ENISA?

Odgovor agencije:

Med ključnimi ugotovitvami poročila Skupine za sodelovanje glede varnosti omrežij in informacij (NIS Cooperation Group) glede napredka držav članic pri izvajanju Sklopa orodij EU za varnost omrežij 5G (EU Toolbox for 5G security) (v nadaljevanju; Drugo poročilo NIS CG) glede implementacije strateških ukrepov, ki se nanašajo na dobavitelje z visokim tveganjem je bilo med drugim izpostavljeno, da naj države članice pri oceni profila tveganja dobaviteljev, upoštevajo kriterije priporočene v Sklopu orodij EU za varnost 5G, saj je očitno, da so med dobavitelji 5G opreme očitne razlike v njihovih značilnostih, zlasti kar zadeva verjetnost vpliva nanje s strani določenih tretjih držav, katerih varnostna zakonodaja in korporativno upravljanje sta potencialno tveganje za varnost Unije. Poročilo državam jasno nalaga da morajo za učinkovito zmanjšanje tveganj zagotoviti, da se posebne omejitve nanašajo tako na kritične kot tudi zelo občutljive elemente omrežja, opredeljene v Usklajeni oceni tveganj, vključno z radijsko dostopovnim omrežjem (RAN).

GZS spraševanje, na podlagi katerih strokovnih podlag se je AKOS odločil uvrstiti RAN med kritične elemente omrežja in kaj so vsebinski razlogi za takšno uvrstitev?

Odgovor agencije:

Agencija je odgovor podala že pri prejšnjih odgovorih.

Na podlagi Zakona o dostopu do informacij javnega značaja je GZS želel še:

Kakršnakoli priporočila URSIV ali drugo korespondenco, ki jo je prejela agencija v zvezi z obravnavanim predlogom splošnega akta in vso dokumentacijo vezano na pripravo predloga navedenega splošnega akta.

Odgovor agencije:

Agencija sodeluje z URSIV predvsem v obliki delovnih sestankov, na katerih pa se ne vodijo zapisniki pač pa se razpravlja o vseh relevantnih virih za odločanje v tej zadevi in skladno z njimi oblikuje besedilo predloga splošnega akta.

URSIV je Agenciji, v zvezi s problematiko, dne 28. 7. 2023 poslal tudi dokument z oznako INTERNO z naslovom: Priporočilo agenciji pri določanju kritičnih elementov omrežja št. 007-3/2023-1544-18, v katerem predstavi argumente in dokumentacijo za oblikovanje stališča agencije do umestitve določenih kritičnih elementov v predmetni Splošni akt.

Zakon (v nadaljevanju pripombe in mnenja GZS z dne 18. 9. 2023) po mnenju GZS predvideva, da bi morala biti prepoved omejena na »kritične« elemente in funkcije omrežja. Pod tem pojmom se v smernicah EU razume zgolj tako imenovani jedrni del omrežja (core) skupaj z upravljanjem virtualiziranih omrežnih funkcij (NFV) in omrežno orkestracijo (MANO). Z razširitvijo dometa 117. člena ZEKom-2 tudi na nekritične dele omrežja, kot so radijsko dostopovno omrežje (RAN) ter upravljavske sisteme in druge podporne sisteme, pa se po mnenju Združenja pri GZS dejansko širi krog morebitne prepovedi preko okvirov predvidenih v ZEKom-2.

Odgovor agencije:

Agencija je odgovor podala že pri prejšnjih odgovorih GZS.

GZS meni, da se z izločitvijo posameznih subjektov na trgu prepoveduje svobodno nastopanje določenega ponudnika blaga ali storitev, kar pa menijo, da predstavlja očiten primer državnega posega v konkurenco. Izguba konkurence, pa zapišejo, bi gotovo pomenila poslabšanje konkurenčnih razmer na trgu, dvig cen in s tem poslabšanje položaja za potrošnike, obenem pa bi upočasnila razvoj omrežij in negativno vplivala na poslovanje operaterjev. Opozarjajo tudi na visoke stroške, katerim bi bili izpostavljeni operaterji zaradi visokih cen menjav dostopovnega dela omrežja (potencialno več 100 milijonov EUR), in nasploh zvišanjem cen izgradnje in vzdrževanja mobilnih omrežij v prihodnje, kar bi vse imelo negativne vplive na gospodarstvo.

Odgovor agencije:

> Agencija s predmetnim splošnim aktom ne omejuje uporabe opreme konkretnih proizvajalcev ali ponudnikov storitev podpore tretje ravni.

Dodajo še, da bi Slovenija s takšnimi ukrepi postala precedenčni primer v Evropi, kar bi ogrozilo uvajanje tehnologij 5G, zavrlo razvoj informacijske družbe in ogrozilo ambiciozne načrte Slovenije glede strategije razvoja informacijske družbe Republike Slovenije do leta 2030.

Odgovor agencije:

> Predmetni SA določa predvsem kritične elemente omrežja in pripadajoče informacijske sisteme, kot to določa ZEKom-2. Agencija SA kot že rečeno pripravlja v sodelovanju z URSIV, ki je Agenciji, v okviru sodelovalne dolžnosti pripravil tudi Priporočilo pri določanju kritičnih elementov omrežja št. 007-3/2023-1544-18, v katerem predstavi argumente in podlage za določitev kritičnih elementov v predmetnem SA. Z njim se torej zasleduje javni interes za zagotovitev varnih omrežij in posledično storitev kritičnim subjektom. Agencija se zato ne strinja s pripombo, da bo SA ogrozil uvajanje tehnologije 5G.

Zapišejo, da so prejeli pojasnilo agencije, o dokumentaciji, na podlagi katere je agencija pripravila predlog Splošnega akta, vendar pa navedena dokumentacija, na katero se sklicuje agencija (vključno s poročili), jasno razmejuje med kritičnim in nekritičnim delom omrežja.

Odgovor agencije:

Agencija je na to vprašanje že odgovorila zgoraj. SA je nastal v sodelovanju z URSIV, ki je agenciji glede določitve kritičnih elementov omrežja posredoval tudi Priporočilo, ki vsebuje vse potrebne razloge, argumente in podlago.

Predlagajo, da mora biti vsak državni poseg predvidljiv, določen in utemeljen z dejanskimi varnostnimi pomisleki in sorazmeren, ne da bi nerazumno omejevali uvajanje in razvoj omrežja.

Odgovor agencije:

Agencija se z predlogom strinja, temu je namenjeno javno posvetovanje in predhodno obdobje za uveljavitev predmetnega predpisa.

Pozivajo, da Agencija v duhu Resolucije o normativni dejavnosti (ReNDej) natančno izdela presojo posledic predlaganega splošnega akta, vključno z morebitnimi zmanjšanjem konkurenčnosti, visokimi stroški regulatornih omejitev in da upošteva tudi ogroženost ambicioznih načrtov Republike Slovenije glede digitalne strategije in razvoja informacijske družbe in zmanjšanjem konkurenčnosti gospodarstva Republike Slovenije zaradi ovir pri uvajanju novih tehnologij.

Odgovor agencije:

Agencija je pri pripravi SA vse navedeno upoštevala v največji možni meri.

II. Pripombe, predlogi in mnenja Telemach odgovori AKOS

Pri Telemach menijo, da ne obstajajo spremenjene okoliščine in dejstva, ki bi podpirale objavo novega predloga akta na način, kot je to storila agencija. Pri tem pojasnjujejo, da naj bi agencija pripravila Splošni akt v luči sprememb na evropski in nacionalni ravni in na podlagi dejstev in ugotovitev, ki izhajajo iz priporočila Urada Vlade za informacijsko varnost (URSIV). Agenciji očitajo, da ne razkriva, informacij o konkretnih dogodkih in dokumentov, ki so bili podlaga za odločitev. Menijo, da gre za pristop, ki nasprotuje načelom 1, 2, in 3. člena Ustave RS (načelo demokratičnosti, pravne države in delitve oblasti) iz katerih izhajata obveznosti delovanja izvršilne veje oblasti na vsebinski podlagi in v okviru zakona. Agenciji očita spreminjanje oziroma originarnega (izvirnega) urejanja zakonske

materije s podzakonskimi predpisi. Dodajajo, da je naloga agencije iskanje ravnovesja med različnimi interesi, na eni strani trga in na drugi varnosti, v nasprotnem primeru, da bi lahko URSIV samostojno sprejemal akte zgolj v prid interesom varnosti.

Odgovor agencije:

> Agencija je že zgoraj pojasnila pravno naravo priporočila URSIV (označba dokumenta s stopnjo tajnosti), navedla pa je tudi evropske dokumente in druge akte, ki jih je prav tako upoštevala pri pripravi SA in pri tem ravnala v okvirih zakonskih pooblastil.

Iz določb ZEKom-2 izvedejo zaključek, da 1. odstavek 116. člena ne zajema regulacije na področju elektronskih komunikacijskih storitev, ker da člen nikjer ne omenja storitev temveč zgolj komunikacijska omrežja. Ta isti člen pa je tudi podlaga za določitev kritičnih elementov. Iz zapisanega sledi, ker se storitve izvajajo preko RAN (kritični element) in 116. člen ne omenja storitev v njem ni podlage za uvrstitev RAN pod kritične elemente. Gre za problematizacijo zakonske ureditve materije.

Odgovor agencije:

> S predmetnim SA se določijo kritični elementi omrežja in pripadajoči informacijski sistemi. RAN je del/element omrežja. Agencija ga je skupaj z URSIV prepoznala kot kritični element.

Pojasnjujejo, da vse domače in tuje strokovne podlage, ki jih v zvezi z vključitvijo RAN med kritične elemente navaja agencija, podpirajo ravno nasprotne zaključke, torej, da RAN ne spada med kritične elemente, tako da ne obstoji, niti pravna niti tehnična podlaga za tovrstno odločitev, razen populistično-političnih izjav komisarja Bretona.

Odgovor agencije:

> Agencija je na to pripombo že odgovorila zgoraj, pri odgovorih GZS.

V tretji točki opišejo metodologijo za ocenjevanje tveganj, ki bi jo bilo potrebno izvesti za kakršenkoli zaključek, kateri elementi so lahko opredeljeni kot kritični.

Odgovor agencije:

Agencija je SA kot že pojasnjeno pripravila skupaj z URSIV in pri tem upoštevala vse relevantne pravne podlage.

Pojasnijo, da svetovno sprejeti standardi informacijske varnosti predlagajo metodo ocene tveganj in ukrepov za njihovo obvladovanje. Primer NIST SP 800-53 predstavi korake v procesu ocenjevanja tveganj in sprejetih ukrepov. ETSI/3GPP standard TR 121 915 pa uvaja klasifikacijo omrežnih elementov na podlagi analize tveganj. Splošni akt pa, da to klasifikacijo spreminja, vendar brez izvedene ocene tveganj. Spremenjena klasifikacija, ki ne vključuje opravljene ocene tveganja pa predstavlja nerazumljiv, celo nestrokoven odmik od dobre prakse ali priporočil EU ali ENISE.

Odgovor agencije:

Agencija se ne strinja z oceno Telemacha, da je odločitev nestrokoven odmik od dobre prakse ali priporočil EU ali ENISA. Pri tem navaja standard ETSI/3GPP TR 121 915 za katerega meni, da jasno razvršča omrežna sredstva glede na stopnjo tveganja. Naveden dokument opisuje funkcije, ki so bile razvite v okviru 3GPP Release 15 verzije, v majhnem delu, na katere se sklicuje Telemach, pa obravnava varnostne aspekte v primeru uporabe NSA ali SA arhitekture oziroma obravnava različne modele zaupanja v primeru scenarijev gostovanja. Tudi omenjen dokument NIST SP 800-53 ni direktno relevanten za nacionalno oceno tveganj držav članic, saj vsebuje zbirko varnostnih kontrol za informacijske sisteme, ki naj jih upoštevajo organizacije, da se zaščitijo pred grožnjami in tveganji, vključno z napadi, človeškimi napakami, naravnimi nesrečami, strukturnimi okvarami, tveganji dobavnih verig in zasebnosti.

Agencija je pri pripravi splošnega akta upoštevala tudi ugotovitve zajete v dokumentu Skupine za sodelovanje glede varnosti omrežij in informacij, EU usklajena ocena tveganj za varnost omrežij 5G, ki obravnava različne scenarije tveganja, grožnje, zlonamerne akterje in ranljivosti, ki so bile prepoznane tako s tehničnega vidika, kot tudi na podlagi nacionalnih ocen tveganj držav članic. Prav tako je med bolj relevantnimi dokumenti, ki obravnavajo varnostno arhitekturo in mehanizme, kot posledično tudi tveganja in kriterije kritičnosti elementov omrežja 5G, tehnična dokumentacija 3GPP TS 33.501 in ostale varnostne 3GPP specifikacije, ki so obravnavane v dokumentu ENISA, Security in 5G Specification, ki je po mnenju agencije bolj relevantna in celovitejša kot dokument ETSI/3GPP TR 121 915.

V četrti točki so opisani pristopi, ki so uporabljeni v Avstriji, Nemčiji, na Finskem in na Madžarskem in ne vključijo RAN med kritične elemente:

- Avstrija ne uvaja opredelitve v zvezi s kritičnimi omrežnimi komponentami.

- Nemčija kritičnih komponent ne opredeljujeta po lastni presoji (Operaterji morajo na podlagi seznama, ki ga zagotovita BSI in BNetzA, določiti, katera komponenta se šteje za "kritično komponento).
- Madžarska ne uvaja opredelitve kritičnih omrežnih komponent ali kakršnih koli omejitev.
- Finska poleg uporabe EU 5G toolbox definicije dodaja seznam, ki ne vključuje RAN.

Odgovor agencije:

Agencija odgovarja, da imajo različne države pri naslavljanju te tematike različne pristope in da je pri tem potrebno upoštevat poleg tehničnih razlogov tudi strateške. Ravno iz tega razloga zakon za pripravo tega SA predvideva sodelovanje agencije in URSIV, da se ustrezno naslovijo vsi aspekti, vključujoč nacionalno varnost.

Telemach pojasnjuje, da deveta točka 1. odstavka 3. člena predloga Splošnega akta določa usmeritve za operaterje pri dobaviteljskih pogodbah, peti odstavek 6. člena pa nalaga izogibanje dolgoročnim pogodbam z dobavitelji. Ti ukrepi po mnenju operaterja presegajo pooblastilo iz 5. odstavka Zakona o elektronskih komunikacijah, ki omejuje regulacijo na »druge zlasti tehnične usmeritve«, kar po mnenju operaterja nasprotje določbi 87. člena Ustave RS.

Odgovor agencije:

Agencija odgovarja, da je pooblastilo agenciji in URSIV dano na podlagi ZEKom-2 in da bi o morebitni prekoračitvi lahko odločalo le Ustavno sodišče.

Telemach pojasnjuje, da je omejevanje konkurence z oblastnimi akti in dejanji prepovedano po Zakonu o preprečevanju omejevanja konkurence. Opozarjajo, da lahko že možnost prepovedi poslovanja z določenim podjetjem vpliva na trg. Opozarjajo, da bi odločitve oblasti morale biti predvidljive in temeljiti na strokovnih kriterijih. Predlagana vključitev RAN med kritično elemente, pa kaže na nepredvidljivost, ki daje trgu signal, da je potrebno sprejeti previdnostne ukrepe, čeprav formali akt še ni bil sprejet. Menijo, da bi to lahko privedlo do višanja cen opreme, daljših dobavnih rokov in omejenega nabora tehnologij, upočasnjenega razvoja sektorja IKT ter zaostanka v digitalizaciji nacionalnega gospodarstva.

Odgovor agencije:

Agencija je na to pripombo že odgovorila zgoraj v odgovorih GZS. Dodatno še odgovarja, da s predmetnim SA ne prepoveduje uporabe nobene specifične opreme, ki bi imela za posledico spremenjene razmere na trgu, kot jih opisuje Telemach. Agencija je pri pripravi SA upoštevala vsa relevantna dejstva, pravne podlage in ustrezna priporočila ter ravnala v okviru svojih pristojnosti.

Telemach v prilogi št. 2 dodaja 9 vprašanj, ki so povzeta v nadaljevanju:

1. Katere so spremembe na evropski in nacionalni ravni, ki so vplivale na odločitev, da se RAN vključi med kritične elemente?

2. Zakaj je definicija kritičnih sredstev odstopa od predhodnih stališč RS zavzetih v razmerju do EU?

3. Zakaj definicija kritičnih sredstev odstopa od smernic EU?

4. Zakaj predlagana ureditev odstopa od praks nekaterih drugih držav EU?

5. Ali je AKOS naredil poglobljeno analizo presoje posledic SA, vključno z vplivom na konkurenco tako na nivoju operaterjev kot tudi dobaviteljev opreme?

Odgovor agencije:

> Agencija je na vprašanja od št. 1 do 5 že odgovorila zgoraj pri odgovorih GZS na strani 2. Tudi glede zadnjega vprašanja je že pojasnila, da SA ne prepoveduje uporabe specifične opreme, saj agencija za takšen ukrep nima pristojnosti.

6. Ali je AKOS naredil analizo potencialne škode (odškodninske odgovornosti RS) v primeru, da se ukrepi izkažejo za neustavne (upoštevaje mnenje Bardutzky)?

Odgovor agencije:

> Agencija s tem SA izvršuje v predvidenem obsegu svoja zakonska pooblastila. Potencialno škodo oz. odškodninsko odgovornost bo ob izkazanem interesu ugotavljalo sodišče.

7. Ali je AKOS preučil dolžnost predhodne notifikacije splošnega akta po TIRS mehanizmu (po SMT Direktivi)?

Odgovor agencije:

> Ko bo oblikovana končna verzija SA bo agencija izvedla tudi notifikacijo po TRIS mehanizmu.

8. Ali je narejena analiza skladnosti predlaganega SA z vidika prava varstva konkurence?

Odgovor agencije:

Agencija je na to pripombo že odgovorila zgoraj na primer pri odgovorih GZS in na strani 9.

9. Ali je narejena analiza potencialnih kršitev Sporazuma o tehničnih ovirah v trgovini oziroma prava WTO?

Odgovor agencije:

S sprejemom SA se ne diskriminira posameznega proizvajalca, distributerja ali ponudnika storitev podpore tretje ravni kot že pojasnjeno pa bo splošni akt notificiran tudi po postopku TRIS.

III. Pripombe, predlogi in mnenja Telekom Slovenije in odgovori AKOS

Telekom Slovenije predlaga konkretne rešitve v nomo-tehnični obliki predstavljenih rešitev, ki jim sledi obrazložitev k posamezni predlagani spremembi ali dopolnitvi pri čemer pozivajo Agencijo, da v izogib nejasnostim pri normiranju materije upošteva podane predloge.

Predlagane spremembe in dopolnitve Telekoma Slovenije k:

1. členu Splošnega akta (vsebina splošnega akta)

(i)

Telekom Slovenije predlaga, da se v 1. točki 1. člena Splošnega akta ustrezno popravi del besedila, ki se glasi: »…oziroma nosilcem ključnih delov sistema varnosti države (v nadaljnjem besedilu: operaterji)« oziroma, da se izbriše besedilo: »(v nadaljnjem besedilu: operaterji)«.

Obrazložitev:

V 1. točki 1. člena Splošnega akta je v zgoraj navedenem delu vsebinsko neustrezno navedeno (predvidevamo, da gre za napako), da se pojem »nosilci ključnih delov sistema varnosti države« v nadaljevanju Splošnega akta nanaša na operaterje. Predlagamo uporabo drugega primernejšega izraza ali pa brisanje dela, ki se glasi »(v nadaljnjem besedilu: operaterji)« v celoti, saj se v nadaljevanju vsebina Splošnega akta ne nanaša več zgolj na del, ki bi bil vezan le na nosilce ključnih delov sistema varnosti države.

(ii)

Telekom Slovenije predlaga, da se v 1. točki 1. člena Splošnega akta del besedila, ki se glasi:

»…oziroma nosilcem ključnih delov sistema varnosti države...«

spremeni, tako da se glasi:

»…in nosilcem ključnih delov sistema varnosti države…«

Obrazložitev:

Menimo, da je pomensko bolj ustrezno, da se za elemente naštevanja ne uporablja beseda »oziroma«, ampak beseda »in«. S tem se tudi doseže poenotenje besedila naštevanja istih subjektov, ki se uporablja v 2. členu, Splošnega akta (pomen izraza »kritični subjekti«).

(iii)

Telekom Slovenije predlaga, da se v 1. točki 1. člena Splošnega akta del besedila, ki se glasi:

»… zagotavljajo ta omrežja kritičnim subjektom, upravljavcem kritične infrastrukture …«

spremeni, tako da se glasi:

»…zagotavljajo ta omrežja kritičnim subjektom, ki so upravljavci kritične infrastrukture …«.

Dodatno predlagamo, da se v nadaljevanju tudi ustrezno popravijo sklanjatve posameznih kritičnih subjektov.

Obrazložitev:

Predlagano besedilo določa, da se usmeritve nanašajo na operaterje, ki zagotavljajo omrežja (i) kritičnim subjektom, (ii) upravljavcem kritične infrastrukture z drugih področij urejanja kritične infrastrukture (iii) izvajalcem bistvenih storitev, (iv) organom državne uprave in (v) nosilcem ključnih delov sistema varnosti države. Iz predloga je mogoče razumeti, da so »kritični subjekti« ena od naštetih (5) kategorij uporabnikov. Glede na pomen izraza »kritični subjekti«, ki ga opredeljuje 2. člen Splošnega akta, pa le-ta zajema vse štiri kategorije uporabnikov in ne le eno od navedenih (ločenih) kategorij. Predlagamo, da se besedilo spremeni na način, da bo jasno, da se vsebina nanaša na kritične subjekte, ki so upravljavci kritične infrastrukture.

2. členu Splošnega akta (pomen izrazov)

(i)

Telekom Slovenije predlaga, da se drugi odstavek 2. člena Splošnega akta, ki se glasi:

»Ostali izrazi, uporabljeni v tem splošnem aktu, imajo enak pomen, kot ga določa zakon.«

spremeni oziroma dopolni, tako da se glasi:

»Ostali izrazi, uporabljeni v tem splošnem aktu, imajo enak pomen, kot ga določata zakon in Splošni akt o varnosti omrežij, storitev in podatkov.«

Obrazložitev:

Predlog Splošnega akta (samostojno) v prvem odstavku 2. člena določa pomen zgolj treh izrazov, za pomene ostalih pa se sklicuje na zakon (ZEKom-2). V Splošnem aktu pa se poleg izrazov, definiranih v ZEKom-2 uporabljajo tudi določeni izrazi, katerih pomen definira Splošni akt o varnosti omrežij, storitev in podatkov (npr. izrazi razpoložljivost, zaupnost, celovitost, avtentičnost …). Da pomen določenih izrazov ne ostane nedoločen oziroma nedorečen oziroma da ne bo prihajalo do različnih razlag pomena izrazov, se predlagana navedena dopolnitev.

3. členu Splošnega akta (splošne usmeritve)

(i)

Telekom Slovenije predlaga, da se ustrezno opredeli, na koga oziroma na kaj se nanaša pojem oziroma izraz »…s strani tretjih…«, ki je uporabljen v 1. točki prvega odstavka 3. člena Splošnega akta.

Obrazložitev:

Naveden pojem oziroma izraz ni ustrezno definiran oziroma opredeljen.

(ii)

Telekom Slovenije predlaga, da se 7. točka prvega odstavka 3. člena Splošnega akta, ki se glasi:

»7. da uporabljene komponente nimajo znanih aktivno zlorabljenih ranljivosti,«

spremeni oziroma dopolni, tako da se glasi:

»7. da uporabljene komponente nimajo ne odpravljenih znanih kritičnih ali aktivno zlorabljenih ranljivosti,«

Obrazložitev:

Pri vsaki opremi se lahko realno pričakuje, da se bodo odkrile varnostne ranljivosti, ki se bodo lahko tudi aktivno zlorabljale. Pomembno pri tem je, da se vse takšne ranljivosti (čim prej) odpravijo. Prav tako je pomembno, da sistem nima neodpravljenih kritičnih varnostnih ranljivosti, ne glede ali se že aktivno zlorabljajo ali (še) ne in ne samo tistih, ki se že aktivno zlorabljajo. S stališča varnosti je torej pomembno ne samo ali so znane (aktivno zlorabljene) ranljivosti, ampak da so te tudi odpravljene oziroma da je proces njihovega odpravljanja hiter in uspešen.

(iii)

Telekom Slovenije predlaga, da se 8. točka prvega odstavka 3. člena Splošnega akta, ki se glasi:

»8. za vsakega dobavitelja se ocenjuje in upošteva tudi tveganja povezana s pravicami uporabe ključnih tehnologij, ki so potrebne za izdelavo in uporabo opreme in s tem posledično omejitve ali prekinitve pri dobavi opreme, nadomestnih delov ali za storitve podpore tretje ravni,«

spremeni, tako da se glasi:

»8. za vsakega dobavitelja se, glede na podatke, ki so dostopni operaterju, ocenjuje in upošteva tudi tveganja povezana s pravicami uporabe ključnih tehnologij, ki so potrebne za izdelavo in uporabo opreme in s tem posledično omejitve ali prekinitve pri dobavi opreme, nadomestnih delov ali za storitve podpore tretje ravni,«

Obrazložitev:

Operaterji nimamo dostopa do potrebnih podatkov o pravicah uporabe ključnih tehnologij, ki so potrebne za izdelavo in uporabo opreme. Te pravice praviloma predstavljajo poslovno skrivnost dobaviteljev, predmet raznih bi- in multi- lateralnih dogovorov ali pa so kakorkoli drugače omejene (geografsko, na ciljnega kupca, na element omrežja …) in v splošnem javno nedostopne, zato ne moremo ustrezno ocenjevati teh vidikov oziroma jih lahko ocenjujemo v omejenem obsegu in glede na podatke, s katerimi razpolagamo. Operaterji lahko prvenstveno ocenjujemo zgolj tveganja, ki se nanašajo na omejitve ali prekinitve pri dobavi opreme, kar pa je zajeto že pri ocenjevanju v točki 1. in 6. prvega odstavka 3. člena Splošnega akta.

(iv)

Telekom Slovenije predlaga, da se 9. točka prvega odstavka 3. člena Splošnega akta, ki se glasi:

»9. izogibanje enemu samemu dobavitelju, da se prepreči odvisnost ter zagotovi odpornost v primeru kritičnih ranljivosti komponent, katastrofalne okvare omrežja oziroma grožnje za varnost omrežij in storitev kritičnih subjektov s strani tretjih fizičnih ali pravnih oseb javnega ali zasebnega prava.«

spremeni oziroma dopolni, tako da se glasi:

»9. izogibanje enemu samemu dobavitelju, da se zmanjša odvisnost ter poveča odpornost v primeru kritičnih ranljivosti komponent, katastrofalne okvare omrežja oziroma grožnje za varnost omrežij in storitev kritičnih subjektov s strani tretjih fizičnih ali pravnih oseb javnega ali zasebnega prava.«

Obrazložitev:

Predlagamo prilagoditev zapisa glede obveznosti operaterjev pri presoji dobavne verige komponent kritičnih elementov omrežja in storitev podpore tretje ravni.

4. členu Splošnega akta (ocenjevanje tveganosti)

(i)

Telekom Slovenije predlaga, da se bolj jasno opredeli oziroma definira pojem »zmogljivost«, ki se uporablja v 1. točki drugega odstavka 4. člena Splošnega akta v povezavi z vrednotenjem tehničnih vidikov tveganosti dobavitelja.

Obrazložitev:

V 1. točki drugega odstavka 4. člena Splošnega akta se del predlaganega besedila glasi »celotno kakovost (vključno z varnostnimi vidiki) in zmogljivosti«, nikjer pa ni jasno opredeljeno oziroma definirano, na kaj se nanaša pojem »zmogljivost«. Če se beseda nanaša na performančno zmogljivost komponente oziroma kritične elemente omrežja, je to parameter, ki je vezan na izbiro posameznega elementa in (v splošnem) ni vezan na dobavitelja oziroma njegovo tveganost (dobavitelj lahko pomuja performančno bolj in manj zmogljive komponente). Če pa so mišljene kakšne druge zmogljivosti (npr. zmogljivost pravočasne dobave, nadgradnje, odprave napak in ranljivost …) pa se naj to tudi ustrezno navede oziroma opredeli.

(ii)

Telekom Slovenije predlaga, da se bolj jasno opredeli oziroma definira pojem »lastnega upravljanja in vzdrževanja«, ki se uporablja v 7. točki drugega odstavka 4. člena Splošnega akta v povezavi z vrednotenjem tehničnih vidikov tveganosti dobavitelja.

Obrazložitev:

V izogib morebitnim različnim interpretacijam navedene zahteve predlagamo jasno oziroma nedvoumno opredelitev, na kaj se nanaša pojem »lastno upravljanje in vzdrževanje«.

(iii)

Telekom Slovenije predlaga, da se tretji odstavek 4. člena Splošnega akta ustrezno prilagodi, tako da bodo obveznosti operaterjev v povezavi z vrednotenjem netehničnih vidikov tveganosti dobaviteljev jasno in nedvoumno določene.

Obrazložitev:

V tretjem odstavku 4. člena Splošnega akta je veliko nejasnosti, in sicer:

1. točka navedene določbe, ki opredeljuje zmožnost dobavitelja glede varovanja pred nepooblaščenim dostopom do podatkov o prometu in komunikacijskih podatkov, predstavlja (vsebinsko tehnično) zahtevo, ki po vsebini spada med osnovne varnostne zahteve (in ne med dodatne varnostne zahteve), saj lahko operater le tako zagotavlja zaupnost komunikacij;

2. točka navedene določbe opredeljuje zmožnost dobavitelja za neprekinjeno dobavo, ki je (vsaj delno) opredeljena že med usmeritvami oziroma zahtevami v 3. členu Splošnega akta (1. in 6. točka prvega odstavka);

3. točka navedene določbe je zapisana preveč splošno.

5. členu Splošnega akta (splošne usmeritve glede delovanja kritičnih elementov omrežja)

(i)

Telekom Slovenije predlaga, da se v drugem odstavku 5. člena Splošnega akta jasneje opredeli, na katere primere selitve kritičnih elementov omrežja se nanaša določba.

Obrazložitev:

Predlagana določba drugega odstavka 5. člena Splošnega akta operaterjem nalaga, da morajo vsaj 30 dni pred nameravano selitvijo kritičnega elementa omrežja o tem obvestiti Agencijo in organ pristojen za informacijsko varnost. Pri tem pa ni opredeljeno, na katere selitve se nanaša določba (vse / znotraj Republike Slovenije / v Evropsko unijo / izven Evropske unije). Predlagamo, da se jasno opredeli, na katere selitve se nanaša obveznost predhodnega obveščanja. Pri tem predlagamo, da se obveznost nanaša samo na selitve izven držav Evropske unije, v vsakem primeru pa predlagamo, da so iz obveščanja izvzete selitve znotraj Republike Slovenije, saj je nabor kritičnih elementov omrežja (priloga Splošnega akta) takšen, da se selitve znotraj Republike Slovenije (zaradi optimizacij procesov in omrežja) lahko dogajajo zelo pogosto.

(ii)

Telekom Slovenije predlaga, da se v tretjem odstavku 5. člena Splošnega akta jasneje opredeli, na katere primere selitve storitev podpore tretje ravni za kritične elemente omrežja se nanaša določba.

Obrazložitev:

Podobno kot v predlogu k drugemu odstavku 5. člena Splošnega akta, se tudi v tretjem odstavku operaterjem nalaga obveznost obveščanja agencije in organa pristojnega za informacijsko varnost vsaj 30 dni pred selitvijo izvajanja storitev podpore tretje ravni in pri tem ni opredeljeno na katere selitve se določba nanaša (vse / znotraj Republike Slovenije / v Evropsko unijo / izven Evropske unije). Predlagamo, da se jasno opredeli, na katere selitve se nanaša obveznost obveščanja. Pri tem predlagamo, da se obveznost nanaša samo na selitve med državami izven Evropske unije oziroma selitve iz držav Evropske unije v države izven Evropske unije. Opredeli se naj tudi, kako se naj (glede na lokacijo izvajanja storitev podpore tretje ravni) obravnava obveščanje za primere globalnih dobaviteljev, ki imajo svoje podporne centre razporejene globalno in se izvajanje storitev podpore tekom dneva seli med različnimi centri oziroma lokacijami.

8. členu Splošnega akta (pravila glede dostopov in uporabe kritičnih elementov omrežja)

(i)

Telekom Slovenije predlaga, da se 7. točka prvega odstavka 8. člena Splošnega akta, ki se glasi:

»7. se izvaja neizbrisno beleženje dostopov in poskusov dostopov, ki se hrani vsaj 12 mesecev, vključno z varnostno kopijo,«

spremeni tako, da se glasi:

»7. se izvaja neizbrisno beleženje dostopov in poskusov dostopov, ki se hrani vsaj 6 mesecev, vključno z varnostno kopijo, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov,«

ali

»7. se izvaja neizbrisno beleženje dostopov in poskusov dostopov, ki se hranijo toliko časa, kot za tovrstne dogodke določa Zakon o informacijski varnosti za izvajalce bistvenih storitev,«

Obrazložitev:

Trajanje beleženja dostopov je neusklajeno med predmetnim predlogom Splošnega akta (predlog predvideva obdobje hrambe vsaj 12 mesecev), predlogom Splošnega akta o varnosti omrežij, storitev in podatkov (zadnji predlog objavljen 19. 5. 2023 predvideva obdobje hrambe vsaj 6 mesecev) in Zakonom o informacijski varnosti (ZInfV), ki v petem odstavku 12. člena predvideva hrambo za obdobje »šestih mesecev, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov«.

Sicer predlagana določba Splošnega akta velja zgolj za kritične elemente omrežja, v predlogu Splošnega akta o varnosti omrežij, storitev in podatkov pa se določba nanaša na vsa ključna sredstva, vendar pa bi takšno razlikovanje obdobja hranjenja dnevniških zapisov (glede na to ali je nek element/sistem kritični element omrežja ali zgolj ključno sredstvo) pomenilo kompleksnejši sistem hranjenja podatkov in potencialno tudi vzpostavitev dveh takšnih sistemov z različnimi obdobji hranjenja podatkov. Prav tako je nesmiselno, da operaterji hranimo podatke o dostopih za daljše obdobje, kot pa ga ZInfV zahteva za izvajalce bistvenih storitev (zgoraj citirani peti odstavek 12. člena ZInfV) in za organe državne uprave (peti odstavek 17. člena ZInfV).

Predlagamo, da se poenoti obdobje hrambe podatkov v obeh navedenih splošnih aktih, in sicer na način oziroma za obdobje, kot ga določa ZInfV za izvajalce bistvenih storitev. Podredno predlagamo, da se predmetni Splošni akt glede obdobja hrambe sklicuje na relevantno določbo ZInfV. S prenosom direktive NIS2 v nacionalno zakonodajo bodo tudi operaterji namreč postali izvajalci bistvenih storitev.

(ii)

Telekom Slovenije predlaga, da se 8. točka prvega odstavka 8. člena Splošnega akta, ki se glasi:

»8. se izvaja beleženje in nadzor vseh programskih posegov nad komponentami, kjer je to mogoče, vključno s spremembami konfiguracij. Zapisi se hranijo vsaj 12 mesecev, vključno z varnostno kopijo,«

spremeni tako, da se glasi:

»8. se izvaja beleženje in nadzor vseh programskih posegov nad komponentami, kjer je to mogoče, vključno s spremembami konfiguracij. Zapisi se hranijo vsaj 6 mesecev, vključno z varnostno kopijo, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov,«

ali

»8. se izvaja beleženje in nadzor vseh programskih posegov nad komponentami, kjer je to mogoče, vključno s spremembami konfiguracij. Zapisi se hranijo toliko časa, kot za tovrstne dogodke določa Zakon o informacijski varnosti za izvajalce bistvenih storitev,«

Obrazložitev:

Glej predhodno obrazložitev predloga k 7. točki prvega odstavka 8. člena Splošnega akta.

(iii)

Telekom Slovenije predlaga, da se tretji odstavek 8. člena Splošnega akta, ki se glasi:

»(3) Preden operater prenese storitev upravljanja, vzdrževanja ali posodabljanja kritičnih elementov omrežja ali njihovih posameznih komponent na tretjo osebo, preveri in zagotovi, da so pri njej vzpostavljeni vsaj enaki ali boljši varnostni mehanizmi in procesi upravljanja z varnostjo, kot jih ima vzpostavljene sam. O nameri prenosa nemudoma obvesti kritični subjekt ter agencijo in organ pristojen za informacijsko varnost.«

v celoti črta.

Podredno predlagamo, da se navedena določba spremeni tako, da se glasi:

»(3) Preden operater prenese storitev upravljanja, vzdrževanja ali posodabljanja kritičnih elementov omrežja ali njihovih posameznih komponent na tretjo osebo, preveri in zagotovi, da so pri njej vzpostavljeni vsaj enaki ali boljši varnostni mehanizmi in procesi upravljanja z varnostjo, kot jih ima vzpostavljene sam. O nameri prenosa nemudoma obvesti agencijo in organ pristojen za informacijsko varnost.«

Obrazložitev:

Operater lahko izvaja storitve upravljanja, vzdrževanja ali posodabljanja kritičnih elementov omrežja ali njihovih posameznih komponent sam, zanj jih lahko izvaja pogodbeni zunanji izvajalec oziroma lahko te storitve spadajo med storitve podpore tretje ravni. Zadnji stavek tretjega odstavka 8. člena Splošnega akta bi pomenil, da je potrebno obveščanje, če bi te storitve prenesli na tretjo osebo (ki ni izvajalec storitve podpore tretje ravni) pozneje, ne pa takoj ob vzpostavitvi / namestitvi kritičnih elementov omrežja ali posameznih komponent, saj zahteve o obveščanju v tem primeru ni (9. člen Splošnega akta zahteva zgolj obveščanje za izvajanja storitev podpore tretje ravni pa še to zgolj ob uveljavitvi tega Splošnega akta).

Prav tako je v praksi zelo kompleksna izvedba obveščanje vseh deležnikov, kot to predvideva zadnji stavek tretjega odstavka 8. člena Splošnega akta. Ta zahteva obveščanje agencije, organa pristojnega za informacijsko varnost in kritičnih subjektov. Kritični subjekti so (po definiciji izraza v 2. členu tega Splošnega akta) upravljalci kritične infrastrukture, izvajalci bistvenih storitev, organi državne uprave in nosilci ključnih delov sistema varnosti države. Kritičnih subjektov je veliko in niti ni nujno, da so vsi tudi poznani operaterju, prav tako operater nima kontaktov za vsakega od teh kritičnih subjektov, preko katerih bi izvajal obveščanje. Prav tako se bo lahko s prenosom direktive NIS2 v nacionalno zakonodajo število izvajalcev bistvenih storitev povečalo, kar bi pomenilo, da je predlagano obveščanje v praksi neizvedljivo. Menimo, da je zadostno obveščanje zgolj agencije in organa

pristojnega za informacijsko varnost (če je obveščanje sploh smiselno/potrebno), navedena organa pa lahko v nadaljevanju obveščata kritične subjekte.

Odgovor agencije:

> Agencija je vse zgoraj navedene pripombe Telekoma Slovenije ustrezno upoštevala in jih vključila v predmetni SA.

Priloga: Seznam kritičnih elementov omrežja in pripadajočih informacijskih sistemov

Telekom Slovenije predlaga, da se skupine kritičnih elementov omrežja ter posamezne funkcionalnosti omrežja in informacijskih sistemov zapiše bolj jasno, kjer je možno čimbolj skladno s standardi (npr. 3GPP, TMF…) za mobilna omrežja ali pripadajoče OSS, BSS informacijske sisteme.

Obrazložitev:

Glede na pomembnost opredelitev je potrebna in verjamemo, da tudi možna, bolj jasna definicija skupin kritičnih elementov omrežja ter funkcionalnosti omrežja in informacijskih sistemov – npr. uporabi se lahko 3GPP TS 23.501 ali ETSI standard, prav tako pa se lahko sisteme opiše s primeri.

Odgovor agencije:

> Agencija je pri oblikovanju seznama kritičnih elementov sledila konceptu oziroma tabeli v točki 2.21 dokumenta NIS CG, EU usklajena ocena tveganja za omrežja 5G, ki so jo skupaj pripravile vse države članice, za katerega posledično meni, da je ustrezen, zato bo tabela, kot je bila v javnem posvetovanju ostala nespremenjena.

Splošni predlog Telekoma Slovenije

Telekom Slovenije predlaga, da naj Splošni akt dodatno precizira oziroma natančneje določi vloge in zahteve do dobaviteljev opreme ali storitev ter do proizvajalcev opreme.

Obrazložitev:

V osnovi v dobavni verigi ločimo med proizvajalci opreme in dobavitelji opreme ter storitev, zato mora biti v Splošnem aktu jasno določeno ali se vse zahteve oziroma obveznosti enako nanašajo na proizvajalce in dobavitelje ali pa so specifične zahteve vezane le na bodisi proizvajalce bodisi dobavitelje.

Odgovor agencije:

Agencija je »splošni predlog« Telekoma Slovenije upoštevala tako, da je bolj natančno določila, katere zahteve se nanašajo tako na dobavitelje kot tudi na proizvajalce ter ponudnike podpore tretje ravni.

IV. Pripombe, predlogi in mnenja T-2 d.d. in odgovori agencije

T2 predlaga konkretne rešitve v nomo-tehnični obliki predstavljenih rešitev k posamezni predlagani spremembi ali dopolnitvi pri čemer pozivajo agencijo, da v izogib nejasnostim pri normiranju materije upošteva podane predloge, v nadaljevanju predlaganih sprememb in dopolnitev.

K 3. členu (splošne usmeritve)

Predlog splošnega akta v prvem odstavku 3. člena predvideva naslednje usmeritve za operaterje:

da za vsakega dobavitelja izvajajo oceno tveganja z vidika dobave in potencialnih možnih vplivov s strani tretjih, združljivosti z opremo drugih proizvajalcev, kakovosti in varnosti proizvodov in z vidika potencialnih negativnih vplivov na delovanje storitev operaterja in kritičnih subjektov (1. točka prvega odstavka) ter nadalje

da za vsakega dobavitelja se ocenjuje in upošteva tudi tveganja povezana s pravicami uporabe ključnih tehnologij, ki so potrebne za izdelavo in uporabo opreme in s tem posledično omejitve ali prekinitve pri dobavi opreme, nadomestnih delov ali za storitve podpore tretje ravni (8. točka prvega odstavka).

Operaterji sami ne razpolagamo z zgornjimi podatki, potrebnimi za izvedbo ocene tveganja, ter moramo zanje zaprositi dobavitelje. Agenciji predlagamo, da v splošnem aktu določi obveznost dobaviteljem za posredovanje podatkov za pripravo analiz ter kot prilogo splošnega akta določi obrazec za dobavitelje za izpolnitev zahtevanih podatkov.

Predlagajo brisanje 9. točke prvega odstavka 3. člena, ki določa izogibanje enemu samemu dobavitelju. Uporaba opreme različnih dobaviteljev je običajno zaradi tehnične nekompatibilnosti neizvedljiva (npr. »handover« baznih postaj pri opremi različnih dobaviteljev ni izvedljiv. Prav tako bi oprema različnih dobaviteljev zahtevala podvojene investicije, kar pa je finančno nevzdržno.

Drugi odstavek 3. člena določa naslednje:

»Operaterji pri dobavi informacijsko-komunikacijske opreme, sistemov in storitev v celoti upoštevajo smernice Agencije Evropske Unije za kibernetsko varnost (v nadaljnjem besedilu:

ENISA) in veljavnih predpisov Evropske Unije glede osnovnih varnostnih zahtev pri naročanju

varnih proizvodov in storitev s področja informacijsko-komunikacijskih tehnologij (primer: »Indispensable baseline security requirements for the procurement of secure ICT products and

services«; verzija 1.0, december 2016 ali novejša)«.

Predlagajo, da se dokumenti ENISA in predpisi EU navedejo določno. Prav tako predlagamo, da se ob vsaki naknadni objavi dokumenta, ki ga je potrebno upoštevati, spremeni splošni akt.

Odgovor agencije:

Pripombe je agencija smiselno upoštevala tako, da je prilagodila besedilo v 9. točki prvega odstavka 3. člena. V drugih predlogih k 3. členu pa pripomb ni upoštevala, saj nima pristojnosti nad dobavitelji opreme in posledično njim neposredno ne more naložiti nobenih obveznosti. Glede navajanja konkretnih predpisov in smernic v splošnem aktu pa je tudi že pojasnila, da zaradi pogostosti njihovega spreminjanja in dopolnjevanja takšna ureditev ni smiselna. Je pa agencija v SA dodala določilo, da bo na svoji spletni strani relevantne smernice in priporočila ažurno objavljala.

K 4. členu (ocenjevanje tveganosti)

Predlagajo brisanje tretjega odstavka 4. člena, saj tveganja povezana z ne-tehničnimi vidiki predmet urejanja 117.člena ZEKom-2. Operaterji prav tako ne morejo pridobiti verodostojnih podatkov za pripravo ocene tega tveganja.

Odgovor agencije:

Agencija je upoštevala predlog T-2.

K 6. členu (usmeritve glede varnostnih ukrepov)

Predlagajo brisanje petega odstavka 6. člena. Kot že zgoraj pojasnjeno, operaterji zaradi tehničnih razlogov ne morejo uporabljati opreme različnih dobaviteljev.

Odgovor agencije:

Pripombe je agencija smiselno upoštevala tako, da je spremenila besedilo 5. odstavka 6. člena.

V. Pripombe, predlogi in mnenja Huawei d.o.o. ter spremljajoči dokumenti in odgovori agencije

Podjetje je svoje pripombe in mnenja poslalo kot:

- Pripombe in predlogi k predlogu novega »Splošnega akta o dodanih varnostnih zahtevah in omejitvah« vključno z analizo ustavne spornosti predloga splošnega akta.

  Spremljajoči dokumenti:

- Pravno mnenja o skladnosti nekaterih določb, predvidenih v predlogu Splošnega akta o dodatnih varnostnih zahteva in omejitvah, z Ustavo Republike SLO, pripravljeno septembra 2023, s strani Inštituta za primerjalno pravo, pri Pravni fakulteti v Ljubljani, Poljanski nasip 2, 1000 Ljubljana, Slo., pripravil: izr. prof. dr. Samo Bardutzky, univ. dipl. pravnik.
- Nacionalne ocene tveganja RS, s področja kibernetske varnosti
- Odgovor agencije na poslane pripombe Huawei v postopku sprejemanja Splošnega akta
- Popis zadeve iz evidence SPIS vodene za potrebe agencije pri sprejemanju Splošnega akta
- Študija Ekonomske fakultete Univerze v Ljubljani, glede ekonomskega učinka omejevanja konkurence

Huawei izpostavlja, da po določbi petega odstavka 116. člena ZEKom-2 operater mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja določenemu krogu uporabnikov, »v kritičnih elementih in funkcijah tega omrežja in pripadajočih informacijskih sistemih ne sme uporabljati opreme in storitev podpore tretje ravni, katera uporaba bi lahko ogrozila nacionalno varnost.« 117. člen ZEKom-2 daje vladi pristojnost, da z odločbo določi takšno opremo in storitve tretje ravni.

Odgovor agencije:

Agencija odgovarja, da navedba Huawei sicer ni pripomba na SA vendar navedeno drži.

Huawei v zvezi s tem da lahko prekrškovni organ operaterja, ki ne upošteva dodatnih varnostnih zahtev in omejitev iz 116. člena, kaznuje s plačilom globe (25. točka prvega odstavka 299. člena ZEKom-2), opozarja na drugo možno negativno posledico za razlago definicije kritičnih elementov s strani operaterja, ki ne ustreza razumevanju pojma kritičnih elementov s strani agencije, ki celo ni predvidena v zakonu, ampak jo je možno razbrati iz razpisnih pogojev nedavno objavljenega javnega razpisa za dodelitev radijskih frekvenc za zagotavljanje javnih komunikacijskih storitev končnim uporabnikom. V razpisni dokumentaciji je predvideno, da lahko agencija določbo o dodelitvi radijskih frekvenc razveljavi, če »pristojen organ v postopki inšpekcijskega nadzora nad izvajanjem zakonskih

in podzakonskih obveznosti s področja varnosti omrežij ugotovi kršitve«, imetnik frekvence pa jih ne odpravi. Pri tem je povedal, da razveljavitev odločbe o dodelitvi frekvenc lahko pomeni uničujoč udarec za gospodarsko aktivnost operaterja. Alternativna pot odprave domnevne kršitve, pa bi terjala zamenjavo opreme, kar pa prinaša znatne stroške, ki bi zagotovo presegli znesek globe, predvidene v prekrškovnih določbah ZEKom-2. Opozarjajo da se bo lahko operater povsem razumno in ekonomično raje odločil, da sploh ne uporablja opreme, za katero bi bila izdana odločba vlade po prvem odstavku 117. člena ZEKom-2 – torej ne le, da se tej opremi izogne v kritičnih elementih, temveč v celotnem omrežju.

Odgovor agencije:

> Agencija odgovarja, da vsa tveganja, povezana z izbiro in dobavo opreme vedno nosi operater, ki mora pred tem opraviti oceno tveganj skladno s 116. členom ZEKom-2. V primeru, da je določena oprema prestala presojo evropskih certifikacijskih organov, ki izvajajo presojo z vidika varnosti ali kakovosti, se šteje, da je ta oprema tehnično ustrezna brez dodatne presoje s strani operaterja.

Huawei poudarja, da kot izhaja iz Mnenja, povsem možen razvoj dogodkov pokaže, da je državna oblast s kombinacijo prepovedi uporabe opreme oziroma storitev po petem odstavku 116. člena ZEKom-2 in nedoločene definicije kritičnih elementov povsem zaobšla zahtevo po sorazmernosti v povezavi z zahtevo po jasnosti in določnosti predpisov kot element načela pravne države po 2. členu Ustavno sodišče Republike Slovenije (v nadaljevanju: URS). S pomensko odprto definicijo, ki pa je ne bodo imela priložnosti interpretirati sodišča, bo agencija dosegla, da bo de facto učinek odločbe iz prvega odstavka 117. člena ZEKom-2 segel preko dometa, ki ga je predvidel zakonodajalec v prepovedi iz petega odstavka 116. člena ZEKom-2. Zaradi pomensko izredno široke definicije operaterjem zoži prostor za svobodno sprejemanje poslovnih odločitev in posega v svobodno gospodarsko pobudo dobaviteljev.
Huawei poudarja, da je poseg tako intenziven, da bi, če bi bil transparentno predviden v zakonodaji, obenem pa bi bila pooblastila za izvrševanje dana oblastnim organom, ne prestal skladnosti z ustavo – načelom sorazmernosti in načelom jasnosti in določenosti predpisov.

Odgovor agencije:

> Agencija odgovarja, enako kot je že pojasnila zgoraj pri odgovorih Telemach. Za določitev kritičnih elementov omrežja, je agencija v predvidenih zakonskih okvirih upoštevala vse relevantne podlage in usmeritve, k čemur jo zakon tudi zavezuje. Zato so navedbe glede nezakonitega poseganja v svobodno gospodarsko pobudo po mnenju agencije neutemeljene.

Huawei izpostavlja, da iz Mnenja izhaja, da je možno bolj jasno in določno formulirati predpis. V postopku zbiranja informacij in analize stanja je za potrebe ocene tveganja kibernetske varnosti omrežij 5G nastalo poročilo, s katerim so se strinjale države članice EU. V okviru priprave usklajene ocene tveganja je bila opravljena tudi analiza vprašanja, katere ključne elemente (key elements) je

mogoče šteti za kritične (critial), katere pa je po drugi strani moč razvrstiti v druge kategorije občutljivosti (visoka – high in zmerna –moderate), tako so po tej klasifikaciji med državami članicami bazne postaje uvrščene med elemente »visokega tveganja« ne »kritične«. Enako izhaja tudi iz nacionalnega poročila Slovenije o oceni tveganja kibernetskih tveganj v omrežju 5G.

Odgovor agencije:

> Agencija odgovarja, enako kot je že pojasnila zgoraj. Dodatno pojasnjuje, da so se razmere, predvsem geostrateške, od leta 2019, ko je bila analiza tveganja EU izvedena, bistveno spremenile. Na to jasno kažejo tudi spremembe v številnih državah članicah, ki so povzete tudi v Drugem poročilu NIS CG.

Huawei izpostavlja, da bi veliko bolj natančna kategorizacija v postopku analize tveganja zelo verjetno pomeni, da je tudi zavezujoče pravne norme mogoče oblikovati tako, da bodo iz njih naslovniki lažje predvideli pravne posledice in da bi se preširokemu oblikovanju kategorije kritičnih elementov mogoče povsem izginiti (ne bi zaobšli ustavni zahtevi po sorazmernosti).

Huawei poudarja, da je obravnavana definicija kritičnih elementov predmet urejanja v splošnem aktu agencije, torej na podzakonski ravni. Na ravni podzakonskega urejanja pa bi agencija ob zavedanju, da je mogoče splošni akt relativno hitro spremeniti, morala kritične elemente definirati bistveno bolj določno, z upoštevanjem ugotovitev iz analize tveganj.
Huawei izpostavlja da prepoved uporabe opreme in storitev po potem odstavku 116. člena ZEKom-2 posega v ustavno zagotovljeno pravico do gospodarske pobude. Obseg in težo tega posega pa sodoloča obravnavana definicija kritičnih elementov iz SA, zato je treba učinek obeh norm na prizadete pravne subjekte ustavnopravno analizirati v medsebojni povezavi.
Huawei izpostavlja da glede na procesno konstelacijo (prepovedi iz petega odstavka 116. člena ZEKom-2 in definicija kritičnih elementov po SA) lahko zaključi, da pomensko zelo ohlapna definicija kritičnih elementov krši ustavno zahtevo po jasnosti in določnosti predpisov in ne more prestati presoje skladnosti z ustavnim načelom sorazmernosti (prekomerne in neuravnotežene negativne posledice za dobavitelje).

Odgovor agencije:

> Agencija odgovarja, da je na pripombo odgovorila že v zgornjih odgovorih. Za določitev kritičnih elementov omrežja, je agencija v predvidenih zakonskih okvirih ustrezno upoštevala vse relevantne podlage in usmeritve, k čemur jo zavezuje tudi zakon.

Huawei podaja zaključni predlog: v okviru podzakonskega urejanja bi morali zagotoviti bolj jasno in določno formuliranje pravnih norm, s tem pa bistveno višjo predvidljivost za vse prizadete subjekte.
Huawei glede kršitve prava EU in mednarodnega prava poudarja, da bi splošni akt, če bi bil sprejet v takšni vsebini, v povezavi z izdajo kakršnekoli odločbe po 117. členu ZEKom-2, med drugim kršil:

- Načelo enakosti (14. člen Ustave in člen 20 Listine EU o temeljnih pravicah)
- Pravico do zasebne lastnine (33. člen Ustave, 1. člen Dodatnega protokola k Evropski konvenciji o varstvu človekovih pravic)
- Pravico svobodne gospodarske pobude (74. člen Ustave, člen 16 Listine EU) in varstvo konkurence in splošne svobode ravnanja (35. člen Ustave)
- Prepoved diskriminacije (14. In 22. člen Ustave, 14. člen EKČP, člen 21 Listine EU).

Omejevanje glede na državo izvora (kriteriji iz prvega odstavka 117. člena ZEKom-2) bi bilo v nasprotju z načeli nediskriminacije in sorazmernosti (Ustava RS, Pogodbe EZ, Listina EU). Iz navedenega je najbolj problematično, če omejevanje sploh ne bi bilo jasno zamejeno in bi se raztezalo tudi na elemente in sredstva, ki ne štejejo za kritične po Usklajeni oceni tveganj in Nacionalni oceni tveganj RS. Prepoved, ki temelji na državi izvora dobavitelja opreme, bi kršila tudi načeli največjih ugodnosti in nacionalne obravnave, sta ključni v skladu s pravom WTO in veljavnimi bilateralnimi investicijskimi sporazumi. Nazadnje bi bil poskus izključitve ali omejevanja možnosti dobaviteljev opreme glede na sedež pri prodaji 5G v EU ne produktiven, vse še toliko bolj, če bi se prepoved nanašala tudi na nekritična sredstva (dostopovni del omrežja – RAN). Splošni akt, ki bi v povezavi s 117. členom ZEKom-2 pripeljal do tega, da bi se prepovedalo tudi dostopovno omrežje in celo pasivna oprema, ki nikakor ne more biti kritična v smislu kibernetske varnosti, nikakor v nobenem primeru ne more prestati testa sorazmernosti.

Huawei meni, da bi sprejem predmetnega predloga SA pomenila veliko negotovost, ki bi pomenila, da se lahko praktično kadarkoli zgodi, da se določen dobavitelj izključi iz trga. Negotovost bi negativno vplivala tako na izbor dobaviteljev in posledično na razvoj področja. To bi lahko imelo velik vpliv na tako na povečanje naložbenih stroškov kot tudi hude posledice za gospodarstvo in potrošnike.

Huawei meni, da bi sprejem predmetnega predloga SA, negativno vplivala na tehnološko rast, inovacije, gospodarsko rast in druge parametre gospodarstva, kar dokazujejo s študijo Oxford Economics in študijo o Ekonomskih učinkih omejevanja konkurence pri ponudbi 5G tehnologije na slovensko gospodarstvo.

Odgovor agencije:

> Agencija odgovarja, da s predmetnim SA, kot je že večkrat pojasnila, ne prepoveduje uporabe opreme kateregakoli dobavitelja. Agencija s SA določa predvsem kritične elemente omrežja. Operaterjem je v zvezi z izvrševanjem predmetnega SA omogočeno tudi prehodno obdobje za prilagoditev in uskladitev. Morebitno prepoved uporabe opreme bo vpeljal akt izdan po postopku in na podlagi 117. člena ZEKom-2. Za prilagoditev na morebitne takšne omejitve pa tudi v tem primeru 312. člen ZEKom-2 določa prehodno obdobje, ki omogoča operaterju uporabo opreme, do konca njene življenjske dobe, vendar najdlje še sedem let od objave informacije o izdani odločbi po prvem odstavku 117. člena ZEKom-2.

Huawei meni, da je definicija kritičnih sredstev preširoka in zajema elemente, ki niso kritični ter da definicija v tej obliki tudi nasprotuje URS kot to izhaja iz poslanega mnenja (spremljajoči dokumenti).

Odgovor agencije:

> Agencija odgovarja, enako kot je že pojasnila zgoraj in dodaja, da je presoja kritičnosti elementov v pristojnosti pripravljavcev tega akta, torej agencije in URSIV.

Huawei meni, da bi bilo omejevanje glede na državo izvora v nasprotju z načeli ne-diskriminacije in sorazmernosti kot to izhaja iz URS.

Odgovor agencije:

> Agencija odgovarja, enako kot je že pojasnila zgoraj, da namen SA ni diskriminacija glede na državo izvora in da predmetni SA tega ne vsebuje.

Huawei problematizira ustavno spornost (87. člen URS) splošnega akta, upoštevaje testa nujnosti in sorazmernosti in prekoračitve zakonskega pooblastila iz ZEKom-2, v delu določanja vsebine pravnih poslov, ki jih bodo operaterji sklepali z dobavitelji, ker ne gre zgolj za določitev: »drugih zlasti tehničnih usmeritev«.

Odgovor agencije:

> Agencija odgovarja, enako kot je že pojasnila zgoraj, (da je pooblastilo Agenciji in URSIV dano na podlagi ZEKom-2) in da bi o morebitni prekoračitvi lahko odločalo le Ustano sodišče.

Pod točko pet Huawei opozarja na spornost ne tehničnih kriterijev.

Odgovor agencije:

> Agencija odgovarja, da je na pripombo odgovorila že v zgornjih odgovorih. Za določitev kritičnih elementov omrežja, je agencija v predvidenih zakonskih okvirih ustrezno upoštevala vse relevantne podlage in usmeritve, k čemur jo zavezuje tudi zakon.

V točki sedem Huawei problematizira veljavnost Sklepa vlade RS z dne 22. 6. 2023 zaradi ne-objave v Uradnem listu RS.

Odgovor agencije:

Agencija odgovarja, enako kot je že pojasnila zgoraj oziroma, da o veljavnosti sklepov, tudi predmetnega, odloča pristojno sodišče.

Huawei se, v točki osem, opredeli do postopkovnih kršitev agencije pri sprejemanju SA, ki da »obremenijo« javno posvetovanje. Očita ji kršitev Statuta agencije in Uredbe o upravnem poslovanju.

Odgovor agencije:

Agencija je svoj odgovor na vprašanje podala že v uvodu oziroma odgovarja, da agencija sodeluje z URSIV predvsem v obliki delovnih sestankov, na katerih ne nastajajo zapisniki, pač pa se razpravlja o vseh relevantnih virih za odločanje v tej zadevi in skladno z njimi oblikuje besedilo predloga akta. Agencija še sporoča, da je namen vključevanja javnosti v postopke sprejemanja akta prepoznava interesov in predlogov deležnikov, da pa Agencija odločitve sprejema samostojno (230. člen ZEKom-2).

V 8. točki Huawei povzema odgovore agencije na njihova vprašanja, z dne 16. 8. 2023. Dopolnitev podanih odgovor pa Agencija podaja v tem dokumentu.

V 9. točki Pripomb in predlogov k predlogu novega »Splošnega akta o dodanih varnostnih zahtevah in omejitvah Huawei predlaga:

1. Črtanje pete in šeste vrstice priloge SA.

Odgovor agencije:

Predloga Agencija ni upoštevala iz že navedenih razlogov.

2. Črtanje 9. točke prvega odstavka tretjega člena SA.

Odgovor agencije:

Agencija odgovarja, da se s pripombo ne strinja in je pri pripravi končnega besedila splošnega akta ne bo upoštevala, saj se z navedeno določbo implementira strateški ukrep SM05 iz Nabora orodji za 5G varnost (5G Toolbox).

3. Črtanje 6. in 7. člena, ki da presegajo zakonsko pooblastilo.

Odgovor agencije:

Agencija se s pripombo ne strinja, saj člena urejata pomembne zahteve za zagotavljanje varnosti omrežij, preko katerih se zagotavljajo storitve kritičnim subjektom.

4. Črtanje tretjega odstavka 4. člena.

Odgovor agencije:

Agencija je pripombo upoštevala.

5. Črtanje 1, 6, točke prvega odstavka 3. člena SA.

Odgovor agencije:

Agencija se s pripombo ne strinja in je zato pri pripravi končnega splošnega akta ne bo upoštevala, saj navedeni točki v 3. členu urejata pomembne zahteve za zagotavljanje varnosti omrežij, preko katerih se zagotavljajo storitve kritičnim subjektom.

6. Črtanje 8. točke iz prvega odstavka 3. člena SA.

Odgovor agencije:

Agencija se s pripombo strinja in jo je pri pripravi končnega splošnega akta upoštevala.

7. Črtanje 4. točke iz prvega odstavka 3. člena SA besedila »ter njihova neprekinjena dobava«.

Odgovor agencije:

Agencija odgovarja, da se s pripombo ne strinja in je zato pri pripravi končnega besedila splošnega akta ne bo upoštevala, saj navedena točka v 3. členu urejata pomembne zahteve za zagotavljanje varnosti omrežij, preko katerih se zagotavljajo storitve kritičnim subjektom.