

## **AKOS - Agencija za komunikacijska omrežja in storitve Republike Slovenije**

### **Stegne 7**

#### **1000 Ljubljana**

Ljubljana, 18. 9. 2023

### **ZADEVA: Predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (št. 0073-3/2023) in predlog GZS**

Spoštovani,

ena od osnovnih nalog Gospodarske zbornice Slovenije, kot reprezentativnega predstavnika slovenskega gospodarstva, je zastopanje in zaščita interesov poslovnih subjektov na nacionalni, regionalni in panožni ravni in skrb za lokalno poslovno okolje in vpliv na njegovo regulativno izboljšanje. Zaradi izvozne naravnosti slovenskega gospodarstva, in s tem odvisnosti od uravnoteženih in jasnih pravil mednarodnega poslovanja, je področje internacionalizacije deležno naše posebne skrbi in angažiranja. Za slovensko gospodarstvo je prost dostop do tujih trgov ključnega pomena za realizacijo poslovnih načrtov in krepitev mednarodne konkurenčnosti. Delimo interes in skrb za enakopravno in varno poslovanje slovenskih podjetij v tujini, enako kot to pričakujejo tuji poslovni subjekti, ko poslujejo v Sloveniji. Zato podpiramo ukrepe in dejanja, ki zasledujejo te cilje, kot konstruktivni sogovornik pa izražamo in prenašamo tudi priporočila in pričakovanja slovenskega gospodarstva v zvezi z urejanjem in lajšanjem poslovanja na vseh področjih, tudi mednarodnem.

Obenem veliko pozornost posvečamo tudi razvoju informacijske družbe in spodbujanju digitalne preobrazbe Republike Slovenije, vključno z razvojem komunikacijskih omrežij.

Eden od naših pomislekov se nanaša na predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah (št. 0073-3/2023), ki ga je Agencija dne 7.8.2023 objavila na svoji spletni strani in v zvezi s katerim poteka javno posvetovanje. V sodelovanju z našo Sekcijo za kibernetsko varnost ugotavljamo, da navedeni predlog splošnega akta predstavlja velik in bistven odstop od dosedanjih izraženih stališč Republike Slovenije, kot tudi od smernic EU (med drugim vključno z Naborom orodij EU za kibernetsko varnost - EU toolbox on 5G Cybersecurity<sup>1</sup>, Usklajeno oceno tveganj za kibernetsko varnost omrežij 5G - EU Coordinated risk assessment of the cybersecurity

---

<sup>1</sup> Glejte stran 39 od 40, ki definira, da so samo jedrne omrežne funkcije skupaj z upravljanjem virtualiziranih omrežnih funkcij (NFV) in omrežno orkestracijo (MANO) kritični elementi omrežja, preostali elementi: npr. radijsko dostopovno omrežje, upravljaljski sistemi in drugi podporni sistemi pa ne.

of 5G networks<sup>2</sup> in tudi mednarodnih standardov (npr. 3GPP<sup>3</sup>). Namreč splošni akt, v primeru izdaje odločbe vlade po prvem odstavku 117. člena Zakona o elektronskih komunikacijah (ZEKom-2), dejansko določa obseg prepovedi uporabe opreme določenih dobaviteljev, za katere bi bila izdana odločba vlade, v mobilnih komunikacijskih omrežjih (skladno s petim odstavkom 116. člena ZEKom-2). Zakon pri tem 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 upravljalvske sisteme in druge podporne sisteme, pa se dejansko širi krog morebitne prepovedi preko okvirov predvidenih v ZEKom-2. Sprejetje predpisa, t.j. splošnega akta kot je predlagan, s katerim se omejuje ali prepoveduje svobodno nastopanje na trgu določenega ponudnika blaga ali storitev (glede radijskega dostopovnega omrežja), predstavlja več kot očiten primer državnega posega v konkurenco na trgu. Izguba konkurence 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. Operaterji bi bili izpostavljeni tudi potencialnim zelo visokim cenam menjav dostopovnega dela omrežja (potencialno več 100 milijonov EUR), ki ne more šteti za kritično z varnostnega zornega kota, in nasploh zvišanjem cen izgradnje in vzdrževanja mobilnih omrežij v prihodnje, kar bi vse imelo negativne vplive na gospodarstvo. S tem bi se Slovenija tudi oddaljila od dobrih praks in priporočil na ravni EU, mednarodnih standardov (npr. 3GPP), kot tudi od dosedanjih stališč Republike Slovenije (na primer nacionalne ocene tveganj Republike Slovenije<sup>4</sup>), pa tudi dobrih praks na primer Nemčije, Avstrije, Finske in drugih evropskih držav. Slovenija bi tako s takšnimi ukrepi postala precedenčni primer v Evropi, navedeno pa bi ogrozilo uvajanje tehnologij 5G, zavrlo razvoj informacijske družbe in ogrozilo ambiciozne načrte Slovenije glede strategija razvoja informacijske družbe Republike Slovenije do leta 2030.

Prejeli smo tudi pojasnilo Agencije<sup>5</sup>, o dokumentaciji, na podlagi kateri 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 (kamor se prišteva radijsko dostopovno omrežje ter upravljaljskimi sistemi in drugimi podpornimi sistemi) in ne nudijo opore stališču, da bi bilo radijsko dostopovno omrežje kritični del omrežja.

Izpostavljamo, da bo Splošni akt kot regulatorni okvir v prvi vrsti bistveno posegal v poslovanje operaterjev v Sloveniji. Očitno preširok domet definicije kritičnih elementov omrežja, v povezavi

---

<sup>2</sup> Navedena usklajena ocena tveganj določa enako kot Nabor orodij EU za kibernetično varnost, radijsko dostopovno omrežje, upravljaljski sistemi in drugi podporni sistemi, transport in prenosne funkcije pa niso opredeljeni kot kritični (za razliko od jedrnega dela omrežja). Glejte tabelo na strani 16-17.

<sup>3</sup> Glejte na primer standard 3GPP TR 21.915 verzija 15.0.0

<sup>4</sup> Glejte dokument »National 5G Cybersecurity Risk Assessment of the Republic of Slovenia«, ki ga je Republika Slovenija posredovala v okviru priprave usklajene ocene tveganj na ravni EU, stran 10, kjer tabela jasno prikazuje, da je jedrni del omrežja opredeljen kot kritičen, dostopovno omrežje, transport in prenosne funkcije pa ne.

<sup>5</sup> Odločba številka: 090-28/2023/2 z dne 8. 9. 2023 na podlagi Zakona o dostopu do informacij javnega značaja

z možnostjo izključitve dobaviteljev, omejuje razvoj omrežja, poslovne načrte, investicijske cikle in onemogoča operaterjem, da bi svobodno vključili proizvajalce opreme v iskanje najboljših tehnoloških rešitev za svoje omrežje, njihove uporabnike, strateške cilje digitalizacije in gospodarske rasti. Namesto da bi na podlagi objektivnih in nediskriminatornih meril preverjali dejansko ustreznost dejanske opreme in s tem varnost omrežij in storitev, lahko merila vezana na državo izvora (npr. 117. člen vsebuje sklicevanja na zakone tretje države, njene zmogljivosti, povezave, ki jih ima vlada te države, itd.) v povezavi s preširoko definicijo kritičnih elementov in funkcij omrežja, privedejo do izjemno hudih posledic za Republiko Slovenijo in njeno gospodarstvo. Tak mehanizem omogoča prepoved uporabe opreme določenega dobavitelja v radijskem dostopovnem omrežju (torej delu omrežja, ki ni kritičen z varnostnega vidika) tudi v odsotnosti kakršnega koli dejanskega vpliva na varnost telekomunikacijskih omrežij. Novi predlog splošnega akta je pri tem v primerjavi s predhodno verzijo iz aprila 2023 še bolj invaziven in še bolj problematičen (predhodni predlog se je omejeval zgolj na bazne postaje (5G ali višje), katerih sevalno območje sega na območje objektov kritične infrastrukture, sedanji predlog pa zajema vse bazne postaje (5G ali višje), kar je še bolj radikalen poseg).

V vsakem primeru predlagamo, da je vsak državni poseg predvidljiv, določen in utemeljen z dejanskimi varnostnimi pomisleki in sorazmeren, ne da bi nerazumno omejevali uvajanje in razvoj omrežja. Če iz objave predloga razberemo, da se zasleduje namen zaščite komunikacij posebnih kategorij, npr. izvajalcev nalog zaščite in reševanja, vojske in podobno, bi se navedeni cilj lahko zasledoval (v duhu sorazmernosti) z navedbo opreme (nejavnih) namenskih omrežij, ki jih takšni subjekti uporabljajo, namesto, da se posega v celoten sistem javnih komunikacijskih omrežij, preko katerih se zagotavljajo storitve splošni javnosti.

Zato predlagamo AKOS, da glede opredelitve kritičnih elementov in funkcij omrežja sledi smernicam EU in dobrim praksam iz tujine in poda jasno razmejitev med jedrnim delom omrežja in preostalimi deli, vključno z radijskim dostopovnim omrežjem ter drugimi sistemi, ob tem pa tudi v duhu Resolucije o normativni dejavnosti (ReNDej) natančno izdela presojo posledic predlaganega splošnega akta, vključno z morebitnimi zmanjšanjem konkurenčnosti, visokimi stroški regulatornih omejitev, ki ne bi imeli podlage v kakršnemkoli dejanskem vplivu na varnost omrežij, 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.

V pričakovanju upoštevanja naših predlogov v dobro slovenskega gospodarstva in družbe vas lepo pozdravljamo.

Gospodarska zbornica Slovenije  
Združenje za informatiko in telekomunikacije

Mag. Nenad Šutanovac, direktor

