**PRIJEDLOG**

U skladu s člankom 116. stavkom 6. Zakona o elektroničkim komunikacijama (UL RS br. 130/22 i 18/23 — ZDU-1O), Agencija za komunikacijske mreže i usluge Republike Slovenije, uzimajući u obzir postupak obavješćivanja u skladu s Direktivom (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva (SL L 241, 17.9.2015., str. 1.), izdaje sljedeće:

# OPĆI AKT
# o dodatnim sigurnosnim zahtjevima i ograničenjima

## Članak 1.
## (Sadržaj općeg akta)

Ovim općim aktom utvrđuje se sljedeće:

1. smjernice kojih se moraju pridržavati operatori pokretnih komunikacijskih mreža (dalje u tekstu „operatori”) koji te mreže pružaju kritičnim subjektima koji su upravitelji kritične infrastrukture u drugim područjima regulacije kritične infrastrukture, kako je utvrđeno u zakonu kojim se uređuje područje kritične infrastrukture (u daljnjem tekstu: „upravitelji kritične infrastrukture”), pružatelji ključnih usluga kako je utvrđeno zakonom kojim se uređuje informacijska sigurnost (dalje u tekstu „pružatelji ključnih usluga”), tijela državne uprave kako je utvrđeno zakonom kojim se uređuje informacijska sigurnost (dalje u tekstu „tijela državne uprave”) ili nositelji ključnih dijelova sigurnosnog sustava zemlje; i
2. kritični elementi mreže i povezanih informacijskih sustava sa svojim funkcionalnostima iz članka 116. stavka 6. Zakona o elektroničkim komunikacijama (UL RS br. 130/22 i 18/23 — ZDU-1O; dalje u tekstu „Zakon”), kako je utvrđeno u prilogu, koji je sastavni dio ovog općeg akta i sastavljen je u suradnji s tijelom nadležnim za informacijsku sigurnost.

## Članak 2.
## (Značenje pojmova)

(1) Pojmovi koji se upotrebljavaju u ovom općem aktu imaju sljedeće značenje:

1. lanac opskrbe je cijeli sustav procesa, ljudi, organizacije i distribucije uključenih u projektiranje, proizvodnju, skladištenje, distribuciju i opskrbu, kao i postavljanje i održavanje komponenata kritičnih elemenata mreže instaliranih u mreži operatora ili kod pružatelja usluga u oblaku koji pruža takve usluge operatoru;

2. ključni elementi mreže su mrežni elementi, funkcije, usluge i popratni informacijski sustavi u fizičkom, softverskom ili virtualiziranom obliku kod operatora ili pružatelja usluga u oblaku, kako je navedeno u prilogu ovom općem aktu;

3. kritični subjekti su upravitelji kritične infrastrukture u drugim područjima regulacije kritične infrastrukture utvrđeni u skladu sa zakonom kojim se uređuje područje kritične infrastrukture, pružatelji ključnih usluga kako je utvrđeno zakonom kojim se uređuje

informacijska sigurnost, tijela državne uprave određena zakonom kojim se uređuje informacijska sigurnost i nositelji ključnih dijelova sigurnosnog sustava zemlje.

(2) Ostali pojmovi koji se upotrebljavaju u ovom općem aktu imaju isto značenje kako je definirano zakonom i općim aktom o sigurnosti mreža, usluga i podataka.

**Članak 3.**
**(Opće smjernice)**

(1) Operatori u lancu opskrbe komponenata kritičnih elemenata mreže i usluga podrške treće razine za te komponente uzimaju u obzir barem sljedeće smjernice tijekom cijelog životnog ciklusa tih komponenata:

1. za pojedinačnog proizvođača ili dobavljača i za pružatelja usluga podrške treće razine zbog odnosa i sporazuma s njima, oni provode procjenu rizika u smislu ponude i mogućih učinaka fizičkih ili pravnih osoba treće strane u skladu s javnim ili privatnim pravom (dalje u tekstu „treće strane”), kompatibilnosti s opremom drugih proizvođača, kvalitete i sigurnosti proizvoda te mogućih negativnih učinaka na rad usluga operatora i kritičnih subjekata;
2. da je sigurnost ugrađena i implementirana već u dizajnu te da ugovori uključuju rokove za uklanjanje uočenih ranjivosti;
3. da su ključne sigurnosne značajke (dostupnost, povjerljivost, cjelovitost i autentičnost) osigurane tijekom cijelog životnog ciklusa njihove uporabe;
4. da su sigurnost i njihova nesmetana opskrba zajamčene te je potvrđeno da podržavaju visoka sigurnosna obilježja u skladu s međunarodno priznatim standardima (3GPP) i europskim tehničkim standardima (ETSI);
5. da se smjernice iz točaka od 2. do 4. ovog stavka mogu provjeriti u ugovornoj dokumentaciji s proizvođačem ili dobavljačem;
6. za svakog proizvođača ili dobavljača također se procjenjuju i uzimaju u obzir rizici povezani s pravima uporabe ključnih tehnologija koje su potrebne za proizvodnju i uporabu opreme te rizici povezani s opskrbom opremom, rezervnim dijelovima ili uslugama podrške treće razine;
7. da upotrijebljene komponente nemaju neriješene poznate kritične ili aktivno iskorištavane ranjivosti;
8. izbjegavanje jednog proizvođača ili dobavljača, ako je to tehnički izvedivo i gospodarski održivo, s ciljem smanjenja ovisnosti i povećanja otpornosti u slučaju ranjivosti kritičnih komponenata, katastrofalnog kvara mreže ili prijetnje sigurnosti mreža i usluga kritičnih subjekata od strane trećih fizičkih ili pravnih osoba uređenih javnim ili privatnim pravom.

(2) Pri opskrbi informacijskom i komunikacijskom opremom, sustavima i uslugama operatori u potpunosti poštuju smjernice Agencije Europske unije za kibersigurnost (dalje u tekstu „ENISA”) i važeće propise Europske unije o osnovnim sigurnosnim zahtjevima pri nabavi sigurnih IKT proizvoda i usluga. Agencija na svojim internetskim stranicama objavljuje poveznice na aktualne ENISA-ine dokumente i propise EU-a u navedenom području te ih ažurira.

(3) Pri opskrbi komponentama kritičnih elemenata mreže ili upotrebi usluga u oblaku prednost se daje odabiru komponenata od onih proizvođača ili dobavljača ili usluga od pružatelja usluga u oblaku koje su certificirala tijela za ocjenjivanje sukladnosti koja su akreditirana i, prema potrebi, ovlaštena na temelju članka 60. stavka 3. Uredbe (EU)

2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (dalje u tekstu „Uredba”) za izdavanje europskih kibersigurnosnih certifikata na određenoj razini jamstva, kako je utvrđeno člankom 52. Uredbe.

(4) Za potrebe prethodnog stavka operator provjerava posebno web-mjesto, koje je uspostavila ENISA u skladu s člankom 55. Uredbe, a namijenjeno je informiranju javnosti o europskim programima kibersigurnosne certifikacije, europskim kibersigurnosnim certifikatima i EU izjavama o sukladnosti, uključujući informacije o europskim programima kibersigurnosne certifikacije koji više nisu valjani ili opozvanim i isteklim europskim kibersigurnosnim certifikatima i EU izjavama o sukladnosti te repozitoriju veza na informacije o kibersigurnosti.

**Članak 4.**
**(Procjena rizika)**

(1) Pri utvrđivanju rizika proizvođača ili dobavljača komponenata i pružatelja usluga treće razine za ključne elemente mreže, operator uzima u obzir sljedeće aspekte rizika koje ocjenjuje.

(2) U vrednovanju iz prethodnog stavka operator procjenjuje i uzima u obzir barem:

1. ukupnu kvalitetu (uključujući sigurnosne aspekte) i pouzdanost;
2. razinu uporabe otvorenih standarda i sučelja kojima se sprečava ovisnost i vezanost za proizvode pojedinog proizvođača ili dobavljača (engl. vendor lock-in);
3. usklađenost s priznatim međunarodnim i europskim tehničkim standardima (3GPP, ETSI) i propisima Europske unije te zadanim sigurnosnim postavkama u skladu sa stručnim preporukama (udruga GSMA);
4. razina kompatibilnosti s opremom i mrežnim funkcijama treće strane;
5. sposobnost pružanja nadogradnji i prilagodbi;
6. postupak upravljanja ranjivostima, njihovo otkrivanje i ažurni postupak s ažuriranjima i popravcima;
7. dostupnost i transparentnost dokumentacije u pogledu:
   - ključnih funkcija i informacija o sigurnosti i drugim značajkama komponente i mogućim postavkama, i
   - korišteni softver, uključujući otvoreni kod (Sastavnica — SBOM);
8. razina ovisnosti o uslugama podrške treće razine u upravljanju opremom i njezinu održavanju ako operator te usluge ne obavlja sam sa svojim zaposlenicima;
9. preliminarna ocjena sukladnosti opreme ili subjekta koji bi pružao uslugu podrške treće razine koju daju tijela akreditirana u Europskoj uniji u skladu s europskim programima kibersigurnosne certifikacije, pri čemu se akreditirana tijela objavljuju u *Službenom listu Europske unije*.

(3) Operator dokumentira čimbenike rizika i rezultate procjene rizika za svakog odabranog proizvođača ili dobavljača ili pružatelja usluga treće razine iz stavaka 2. i 3. ovog članka te ih redovito ažurira.

**Članak 5.**
**(Opće smjernice o radu kritičnih elemenata mreže)**

(1) Komponente kritičnih elemenata mreže, njihov rad i zadane postavke ne smiju sadržavati tehničke značajke koje bi mogle negativno utjecati na sigurnost ili rad kritičnih subjekata, među ostalim zbog sabotaže, špijunaže, krađe intelektualnog vlasništva ili terorizma.

(2) Kritični elementi mreže općenito se nalaze u Republici Sloveniji ili, uzimajući u obzir sve sigurnosne rizike i osiguravajući visoku razinu sigurnosnih mjera, ako to nije drugačije utvrđeno primjenjivim propisima, u Europskoj uniji. Operator o svom planiranom premještanju obavješćuje Agenciju za komunikacijske mreže i usluge Republike Slovenije (dalje u tekstu „Agencija") i tijelo odgovorno za informacijsku sigurnost najmanje 30 dana prije premještanja izvan Europske unije.

(3) Usluge podrške treće razine za kritične elemente mreže općenito se pružaju u Republici Sloveniji ili, uzimajući u obzir sve sigurnosne rizike i osiguravajući visoku razinu sigurnosnih mjera, ako to nije drugačije utvrđeno primjenjivim propisima, u Europskoj uniji. Operator obavješćuje Agenciju i tijelo odgovorno za informacijsku sigurnost o planiranom premještanju svojih usluga podrške treće razine najmanje 30 dana prije premještanja izvan zemalja Europske unije.

(4) Provedbom usluga podrške treće razine ne ugrožavaju se sigurnost ni izvršavanje usluga kritičnih subjekata ili nacionalne sigurnosti.

(5) Operator uspostavlja i redovito provodi postupak utvrđivanja kritičnih elemenata mreže. To se mora provoditi najmanje jednom godišnje ili kada se nabavljaju komponente kritičnih elemenata mreže.

(6) Ako pojedinačna komponenta samo djelomično predstavlja kritični element mreže, smatra se dijelom kritičnog elementa mreže.

(7) Operator ažurira popis svih komponenata kritičnih elemenata mreže, njihovih funkcija, lokacija, administratora i upravitelja, njihovih pružatelja usluga podrške treće razine i njihovih proizvođača ili dobavljača. Popis se na zahtjev stavlja na raspolaganje Agenciji i tijelu odgovornom za informacijsku sigurnost.

**Članak 6.**
**(Sigurnosne mjere za opskrbu komponentama kritičnih elemenata mreže)**

(1) Operator mora biti upoznat s cijelim lancem opskrbe i rizicima povezanima s njim, uključujući podizvođače pojedinačnih komponenata kritičnih elemenata mreže, što uključuje i ključeve šifriranja, UICC/eUICC i druge sigurnosne elemente čija bi zlouporaba mogla ugroziti sigurnost kritičnih subjekata.

(2) Operator osigurava da su sigurnosni zahtjevi između operatora i proizvođača ili dobavljača komponenata kritičnih elemenata mreže ili njegovih pružatelja usluga podrške treće razine ugovorno dogovoreni i dokumentirani te da se od proizvođača ili dobavljača zahtijeva da poštuju dogovorene sigurnosne mjere u cijelom lancu opskrbe.

(3) Kako bi se pravovremeno spriječilo da zlonamjerni akteri iskoriste ranjivosti, operator osigurava da se proizvođač ili dobavljač komponenata ključnog elementa mreže ugovorno obveže da će odmah obavijestiti operatora o otkrivenoj ranjivosti i o mjerama za smanjenje rizika te savjetovati o zaštitnim ili korektivnim mjerama koje operator može poduzeti kao odgovor na prijetnju.

(4) Operator najmanje jednom godišnje provjerava primjerenost prava pristupa kritičnim elementima mreže ili ih bez odgode ažurira u skladu s promjenama u organizaciji ili na strani pružatelja usluga podrške treće razine.

(5) Operator sprečava svoju ovisnost o pojedinačnom dobavljaču ili pružatelju usluga treće razine (tj. engl. „vendor lock-in”), ako je to tehnički izvedivo i gospodarski održivo, s ciljem smanjenja ovisnosti i povećanja otpornosti u slučaju ranjivosti kritičnih komponenata, među ostalim izbjegavanjem dugoročnih ugovora s pojedinačnim proizvođačima ili dobavljačima ili pružateljima usluga podrške treće razine ili mogućnosti njihove izmjene s ciljem smanjenja poremećaja u pružanju usluga kritičnim subjektima na najmanju moguću mjeru.

**Članak 7.**
**(Ugovorni uvjeti s proizvođačima, dobavljačima ili pružateljima usluga podrške treće razine)**

Kako bi se osigurala visoka razina sigurnosti, operator u nove ugovorne uvjete s proizvođačima, dobavljačima ili pružateljima usluga podrške treće razine uključuje barem sljedeće:

1. izjavu proizvođača ili dobavljača da komponenta ili njezine zadane postavke nemaju nedokumentirane programe za neovlašteni ulazak u sustav (engl. backdoor) ili negativan učinak na rad kritičnih subjekata;
2. obvezu proizvođača ili dobavljača ili pružatelja usluga treće razine da će zaštititi podatke s kojima se upoznaju tijekom pružanja usluga ili pristupa njima u vezi s pružanjem usluge pristupa;
3. obvezu proizvođača ili dobavljača ili pružatelja usluga treće razine da odmah obavijeste operatora u slučaju kršenja zaštite komunikacijskih podataka ili podataka o prometu koja utječu ili bi mogla utjecati na operatora ili kritične subjekte iz članka 1. točke 1. ovog općeg akta;
4. obvezu proizvođača ili dobavljača ili pružatelja usluga treće razine da odmah obavijeste operatora o svim sigurnosnim incidentima i ranjivostima koji bi mogli utjecati na sigurnost mreže, povezanih usluga ili podataka operatora;
5. obvezu proizvođača ili dobavljača ili pružatelja usluga treće razine da poštuju sigurnosne standarde i pravila koje je utvrdio operator te da poduzmu odgovarajuće sigurnosne mjere kako bi se osigurala sigurnost informacijskih sustava i mreža te podataka operatora ili kritičnog subjekta;
6. sposobnost operatora da u bilo kojem trenutku pregleda okruženja, postupke, sigurnosne mjere i alate kojima se koristi pružatelj usluga podrške treće razine pri pristupu mreži i podacima operatora;
7. odgovornost proizvođača ili dobavljača ili pružatelja usluga podrške treće razine za štetu koja bi bila uzrokovana utvrđenim slabostima ili zlouporabom komponenata kritičnih elemenata mreže, njihovim zadanim postavkama ili tijekom pružanja usluga

podrške treće razine koje je proizvođač ili dobavljač ili pružatelj podrške treće razine zanemario ili namjerno proveo;
8. obvezu redovitog osposobljavanja osoblja proizvođača ili dobavljača ili pružatelja usluga podrške treće razine u području sigurnosti podataka te informacijskih sustava i mreža.

**Članak 8.**
**(Pravila o pristupu kritičnim elementima mreže i njihovoj uporabi)**

(1) Kada fizički ili logički pristupa komponentama kritičnih elemenata mreže, njihovim postavkama i podacima operatora koji su pohranjeni, obrađeni ili izmijenjeni u njima, operator osigurava sljedeće:
1. pristup je strogo ograničen na osobe koje su prethodno ovlaštene;
2. operater upravlja svim radovima na kritičnim elementima mreže koji se izvode na lokaciji ili putem daljinskog pristupa;
3. višestruka provjera autentičnosti provodi se za korisnike kojima su dodijeljene najviše privilegije prava pristupa pojedinim komponentama kritičnih elemenata mreže, njihovim postavkama ili podacima koji su ondje pohranjeni ili obrađeni;
4. svaka ovlaštena osoba kojoj je odobren pristup ima jedinstveni korisnički račun i lozinku;
5. upotrebljavaju se samo lozinke koje se redovito ili odmah mijenjaju u slučaju otkrivene zlouporabe i sadrže najmanje 15 znakova i uključuju velika i mala slova, brojeve i posebne znakove, ako softver to dopušta;
6. koncept nulte tolerancije ili povjerenja primjenjuje se u pristupu ako je to moguće;
7. sigurnost komunikacijske veze ovlaštenog korisnika s pojedinačnim komponentama zaštićena je uporabom šifriranja, uzimajući u obzir najnovija tehnološka dostignuća i najbolje industrijske dobre prakse u području informacijske sigurnosti, ili koju preporučuju etablirane institucije u području informacijske sigurnosti;
8. provodi se neizbrisiva evidencija pristupa i pokušaja pristupa, koja se čuva najmanje šest mjeseci, uključujući sigurnosnu kopiju, a može i dulje, ako analiza upravljanja rizikom i procjena prihvatljive razine rizika pokažu da bi se rizicima trebalo na odgovarajući način upravljati čuvanjem evidencije tijekom duljeg razdoblja;
9. bilježenje i praćenje svih softverskih intervencija na komponentama provodi se gdje je to moguće, uključujući promjene konfiguracije. Evidencija, uključujući sigurnosnu kopiju tih podataka, čuva se onoliko dugo koliko je navedeno u prethodnoj točki;
10. pristup pojedinačnim komponentama i podacima koji su na njima pohranjeni ili obrađeni vremenski je ograničen i otvoren samo za vrijeme potrebnog rada.

(2) U slučaju pristupa osoblja ili zaposlenika pružatelja usluga podrške treće razine pojedinačnim komponentama kritičnih elemenata mreže, oni:
1. upotrebljavaju samo sigurnu posredničku namjensku radnu stanicu (engl. „jump server”) koja podliježe redovitim sigurnosnim provjerama;
2. instaliraju na namjensku radnu stanicu samo apsolutno potrebne alate, komponente i aktivne usluge za pristup drugim resursima na mreži koji su apsolutno potrebni i moraju se ažurirati najnovijim sigurnosnim zakrpama;
3. upotrebljavaju sigurne kriptografske operacije i ključeve na namjenskoj radnoj stanici koja mora biti smještena u mreži operatora i pod njegovom isključivom kontrolom;
4. svaki pristup odobrava i aktivira operator ručno i samo za vrijeme trajanja pristupa;
5. operater fizički kontrolira i bilježi sve pristupe i aktivnosti;

6. upotrebljava dvostruku provjeru autentičnosti i lozinke koje sadržavaju najmanje 15 znakova i uključuju velika i mala slova, brojeve i posebne znakove, a koje se mijenjaju na temelju procijenjenih rizika.

(3) Prije nego što prenese uslugu upravljanja, održavanja ili ažuriranja kritičnih elemenata mreže ili njihovih pojedinačnih komponenata trećoj strani, operator provjerava i osigurava da ima barem iste ili bolje sigurnosne mehanizme i postupke upravljanja sigurnošću u usporedbi sa svojim mehanizmima i procesima. O namjeri prijenosa odmah obavješćuje dotični kritični subjekt, Agenciju i tijelo odgovorno za informacijsku sigurnost.

(4) Operator provjerava stvarno stanje sigurnosnih postupaka prije početka pružanja usluge, a nakon toga najmanje jednom godišnje. Operator vodi evidenciju o internim pregledima i kontrolama pružanja usluga podrške trećim stranama i čuva ih tijekom pružanja usluga i godinu dana nakon njihova raskida, ali ne dulje od pet godina.

„PRIJELAZNE I ZAVRŠNE ODREDBE

**Članak 9.**
**(Prijelazne odredbe)**

(1) Operator obavješćuje Agenciju i tijelo odgovorno za informacijsku sigurnost o postojećim lokacijama kritičnih elemenata mreže u roku od 30 dana od stupanja na snagu ovog općeg akta.

(2) Operator obavješćuje Agenciju i tijelo odgovorno za informacijsku sigurnost o postojećim lokacijama usluga podrške treće razine za kritične elemente mreže u roku od 30 dana od stupanja na snagu ovog općeg akta.

(3) Agencija će prvi put objaviti dokumente iz članka 3. stavka 2. ovog općeg akta danom njegova stupanja na snagu.

**Članak 10.**
**(Stupanje na snagu)**

Ovaj opći akt stupa na snagu tridesetog dana od dana objave u Službenom listu Republike Slovenije, pri čemu operatori mogu upotrebljavati opremu i održavati pružanje usluga podrške treće razine do isteka rokova iz članka 312. stavaka 2. i 3. Zakona.

Br. _____ mag. Marko Mišmaš

Ljubljana, _____ direktor

EVA 2023-3150-0034

**PRIJEDLOG**

**PRIJEDLOG**

Prilog

**Popis ključnih elemenata mreže i povezanih informacijskih sustava:**

| **Kritični elementi mreže** | **Funkcionalnosti mrežnih i informacijskih sustava** |
|---|---|
| Upravljanje pretplatnicima i mehanizmi šifriranja | - Upravljanje sjednicama (govor i podaci),<br>- autentifikacija korisnika i opreme s mrežom,<br>- upravljanje i pohrana ključeva za autorizaciju pretplatnika i mrežnih komponenata (UICC/eUICC, digitalni certifikati/HSM),<br>- funkcije za sigurnu autentifikaciju, zaštitu integriteta komunikacije (šifriranje) i pohranu korisničkih ključeva, mrežnih i upravljačkih komponenata,<br>- upravljanje pravima pristupa. |
| Međusobno povezivanje | - Značajke udomljavanja i sučelja za druge mreže i usluge. |
| Upravljane mrežne usluge | - Registracija i autorizacija mrežnih usluga,<br>- pohrana i obrada komunikacijskih, lokacijskih i prometnih podataka,<br>- izloženost mrežne i mrežnih funkcija vanjskim aplikacijama i uslugama. |
| Upravljanje i orkestracija virtualiziranih mrežnih funkcija (NFV) i orkestracija mrežom (MANO), uključujući infrastrukturu za virtualizaciju | - Upravljačke funkcije orkestracije i konfiguracije NFV-a bez obzira na vrstu provedbe (VM, kontejner, mikrousluge),<br>- virtualizacijske funkcije za provedbu i uporabu NFV-a,<br>- Funkcija sustava za odabir mreže (NSSF). |
| Radijska pristupna mreža | - Bazne stanice koje podržavaju 5G tehnologiju ili noviju. |
| Sustavi upravljanja i drugi sustavi podrške | - Praćenje rada i upravljanja mobilnom komunikacijskom mrežom, uključujući pristupni dio (RAN/O-RAN),<br>- sustavi za otkrivanje sigurnosnih događaja, nepravilnosti, prijetnji i upravljanja njima (sigurnosne funkcije uključujući SIEM/SOAR). |
| Pravno presretanje | - Funkcije pristupa nadležnog tijela komunikacijskom sadržaju i podacima o korisničkom prometu. |