PREDLOG!

Na podlagi sedmega odstavka 115. člena Zakona o elektronskih komunikacijah – (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) izdaja Agencija za komunikacijska omrežja in storitve Republike Slovenije

SPLOŠNI AKT
o varnosti omrežij, storitev in podatkov

I. SPLOŠNI DOLOČBI

1. člen
(vsebina splošnega akta)

Ta splošni akt določa tehnične usmeritve, ki jih upoštevajo operaterji pri oceni tveganj, vsebino varnostne politike ter tehnične in organizacijske ukrepe, ki jih upoštevajo operaterji z namenom zmanjšanja tveganj za varnost omrežij, informacijskih sistemov in podatkov ter usmeritve glede načrtovanja in zagotavljanja neprekinjenega poslovanja.

2. člen
(pomen izrazov)

(1) Izrazi, uporabljeni v tem splošnem aktu, pomenijo:

1. Avtentičnost je pristna in nepotvorjena lastnost omrežja, informacijskih sistemov, shranjenih, obdelanih ali prenesenih podatkov.

2. Celovitost omrežja je zmožnost sistema, da zagotovi določene lastnosti v okviru vnaprej opredeljenih zmogljivosti in funkcionalnosti z namenom, da se zagotovi neprekinjeno delovanje oziroma razpoložljivost.

3. Grožnja je potencialna nevarnost ozirom možen vzrok za varnostni incident, ki bi lahko ob primernih okoliščinah povzročila škodo organizaciji oziroma negativno vplivala na zaupnost, celovitost in razpoložljivost sredstva.

4. Kibernetska grožnja je grožnja skladno z zakonom, ki ureja informacijsko varnost.

5. Kritični subjekti so upravljavci kritične infrastrukture skladno z zakonom, ki ureja kritično infrastrukturo, izvajalci bistvenih storitev, organi državne uprave in ostali zavezanci na podlagi zakona, ki ureja informacijsko varnost in nosilci ključnih delov sistema varnosti države .

6. Ključna sredstva vključujejo elemente in funkcije omrežja, informacijske sisteme v fizični, programski ali kakršni koli virtualizirani obliki pri operaterju ali pri ponudniku storitev v oblaku, katerih odpoved ali zloraba bi imela velik vpliv v smislu velikega števila prizadetih

uporabnikov, daljšega izpada storitev, izgube zaupnosti, razpoložljivosti ali celovitosti omrežja.

7. Ranljivost je obstoj šibkosti arhitekture ali posamezne opreme, procesov, posledica napak v implementaciji ali upravljanju, odsotnosti notranjih kontrol, ki lahko vodi v nepričakovane neželene dogodke, ki lahko ogrozijo varnost omrežij, informacijskih sistemov in storitev.

8. Razpoložljivost pomeni pravočasen in zanesljiv dostop do sredstev, omrežij, storitev, podatkov ali informacij na zahtevo pooblaščenega uporabnika.

9. Sredstvo je vse kar ima določeno vrednost za organizacijo, predvsem pa vključuje strojno in programsko opremo, podatke, omrežno infrastrukturo in ljudi.

10. Tveganje je potencial oziroma verjetnost, da bo dana grožnja izkoristila ranljivost sredstva ali skupine sredstev in tako povzročila organizaciji škodo oziroma negativno vplivala na zaupnost, celovitost in razpoložljivost sredstev ali skupne sredstev.

11. Zaupnost je lastnost shranjenih, prenesenih ali obdelanih podatkov in povezanih storitev, ki zagotavlja, da informacija ni na voljo ali razkrita nepooblaščenim osebam ali procesom.

(2) Preostali izrazi, uporabljeni v tem splošnem aktu, imajo enak pomen kot je določen v Zakonu o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: zakon).

II. SISTEM UPRAVLJANJA VAROVANJA INFORMACIJ IN NEPREKINJENEGA POSLOVANJA

3. člen
(varnostna politika)

(1) Operater vzpostavi informacijsko varnostno politiko, ki obsega najmanj:
1. določitev obsega sistema upravljanja varovanja informacij (v nadaljnjem besedilu: SUVI) in obsega sistema upravljanja neprekinjenega poslovanja (v nadaljnjem besedilu: SUNP),
2. zahteve iz zakona in tega splošnega akta,
3. navedbo tveganj, nevarnosti in groženj, ki bi lahko ogrozile njegovo delovanje,
4. navedbo organizacijskih vlog, odgovornosti in pooblastil zaposlenih za izvajanje ukrepov informacijske varnosti,
5. upravljanje in varovanje informacij, informacijskih sistemov, omrežij ter storitev tako s strani zaposlenih kot tudi pogodbenih partnerjev.

(2) Informacijsko varnostno politiko in ukrepe za obvladovanje tveganj za informacijsko varnost odobri vodstvo, objavi in sporoči zaposlenim ter relevantnim pogodbenim partnerjem.

(3) Poslovodstvo operaterja izkazuje zavezanost in podporo k upravljanju in nenehnemu izboljševanju informacijske varnosti ter izpolnjevanju veljavnih zahtev v zvezi z informacijsko varnostjo.

(4) Informacijska varnostna politika operaterja sledi bistvenim načelom, kot jih določajo relevantni standardi in dobre prakse s področja upravljanja in varovanja informacij ter neprekinjenega poslovanja.

4. člen
(upravljanje s tveganji)

(1) Operater z uporabo dobrih industrijskih praks, priporočil Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA) in mednarodnih standardov s področja informacijske varnosti, s tehničinimi sredstvi in z informacijami iz dostopnih virov vseskozi prepoznava, obravnava, ocenjuje in vrednoti potencialne grožnje, vključno s kibernetskimi in ranljivosti sredstev, informacijskih sistemov in programske opreme.

(2) V okviru upravljanja s tveganji operater prepozna, opredeli in dokumentira:
1. vsa sredstva, poslovne procese in funkcije, ki so pomembne za delovanje javnih komunikacijskih storitev operaterja,
2. informacije in podatke, ki omogočajo ključne poslovne procese in aktivnosti operaterja,
3. verjetnost nastanka posamezne grožnje in vse potencialne negativne posledice v primeru izrabe grožnje, ki bi lahko vplivale na varnost omrežij in informacijskih sistemov, poslovanje operaterja in njegove storitve.

(3) Na podlagi prepoznanih sredstev, poslovnih procesov, informacij in podatkov iz prejšnjega odstavka operater izvede analizo obvladovanja tveganj in na njeni podlagi izvede oceno sprejemljive ravni tveganj ter uvede ustrezne ukrepe za preprečitev ali omilitev neželenih učinkov in zagotovi nenehno izboljševanje teh ukrepov.

(4) Upravljanje tveganj je sestavni del informacijske varnostne politike in se upošteva tako pri implementaciji SUVI kot tudi pri tekočem poslovanju.

5. člen
(minimalni obseg varnostnih ukrepov)

(1) Operater na podlagi izvedene analize znanih in zaznanih tveganj z namenom zagotavljanja visoke ravni varnosti omrežij, informacijskih sistemov in storitev ter zmanjšanja vpliva varnostnih incidentov, sprejme ustrezne varnostne ukrepe.

(2) Varnostni ukrepi iz prejšnjega odstavka morajo biti dokumentirani, pri čemer morajo biti upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo omrežij in informacijskih sistemov.

(3) Pri določanju ciljev varnostnih politik in pri sprejemanju varnostnih ukrepov v največji meri upošteva vsakokrat veljavne smernice ENISA (npr. »Guideline on Security Measures

under the EECC«) ter priporočila Skupine za sodelovanje glede varnosti omrežij in informacij (v nadaljnjem besedilu: Skupina NIS).

(4) Operater na podlagi analize tveganj vseskozi posodablja varnostne ukrepe, kadar nastanejo bistvene spremembe v okviru SUVI ali po težjem ali kritičnem incidentu, vendar najmanj enkrat letno.

6. člen
(vsebina SUNP)

(1) Operater v okviru SUNP ob upoštevanju njegovih lokacij, njegove velikosti in kompleksnosti, pripravi strateški in taktični načrt in postopke za zagotavljanje neprekinjenega poslovanja ter izvede oceno vpliva na poslovanje, ki zajema navedbo možnih dogodkov in varnostnih incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi elementov omrežij, informacijskih sistemov, kadrovskih razlogov, odpovedi oskrbe z energenti, dobave opreme oziroma storitev podpore tretje ravni.

(2) Na podlagi izvedene ocene iz prejšnjega odstavka operater določi minimalno raven neprekinjenega poslovanja tako, da sprejme naslednje ukrepe:
4. določi minimalen nabor in raven javnih komunikacijskih storitev,
5. določi odgovorne osebe z jasnimi vlogami, pooblastili in odgovornostmi,
6. določi primerne in potrebne nadomestne prostore, informacijske sisteme in elemente omrežja,
7. vzpostavi učinkovit proces shranjevanja oziroma varnostnega arhiviranja (po potrebi na potresno varno rezervno lokacijo) in obnove podatkov v primeru izgube ali zlorabe, ki se periodično preverja,
8. izdela načrt kriznega upravljanja v primeru izpada posameznih lokacij, odpovedi informacijskih sistemov ali posameznih elementov omrežja, izpada oskrbe z električno energijo, drugimi viri oziroma odpovedjo lastnih ali zunanjih storitev,
9. izdela načrt za hitro in učinkovito obnovo poslovanja ob motnjah ali prekinitvah,
10. izdela načrt potrebnih sredstev in storitev podpore tretje ravni za namen zagotavljanja neprekinjenega poslovanja.

(3) Operater redno pregleduje izvajanje in učinkovitost ukrepov iz prejšnjega odstavka, analizira pretekle motnje oziroma prekinitve in dokumentira podatke o preventivno izvedenih vajah.

(4) Poslovodstvo operaterja enkrat letno potrdi ustreznost in učinkovitost SUNP. Operater dokumentira sprejete in izvedene postopke in ukrepe iz drugega odstavka tega člena ter jih na zahtevo agencije predloži na vpogled ali jih posreduje.

(5) Operater pri pripravi in izvajanju SUNP na podlagi tega splošnega akta poleg določbe šestega odstavka 115. člena zakona upošteva tudi priporočila ENISA ter Skupine NIS.

7. člen
(dokumentirane informacije)

(1) Operater v zvezi s SUVI in SUNP sprejme najmanj:

1. dokumente, ki opredeljujejo informacijsko varnostno politiko, njene cilje, obseg in način merjenja rezultatov njene učinkovitosti ter način obravnavanja njenih kršitev,
2. dokumente, ki opisujejo postopke za ugotavljanje, ocenjevanje, analizo in obvladovanje tveganj, vključno s tveganji zaradi nepooblaščenega razkritja osebnih podatkov oziroma prometnih podatkov, uporabe šifriranja, kjer je to potrebno in zapise o potrebnih ukrepih za zaščito le-teh,
3. dokumente, ki vsebujejo seznam poslovnih procesov, funkcij, informacij in podatkov, ki so ključna za neprekinjeno poslovanje,
4. seznam in opredelitev kritičnosti sredstev, lastnih in najetih, ki so potrebna za delovanje storitev, in njihovih lokacij ter seznam njihovih skrbnikov in upravljavcev,
5. ažuren načrt fizične in logične arhitekture omrežja ter fizičnih in logičnih povezav z drugimi operaterji,
6. dokumente, ki določajo postopke za upravljanje dostopa do sredstev (omrežij, informacijskih sistemov in naprav ter spreminjanja njihovih nastavitev), in sicer postopke za dodeljevanje in odvzemanje uporabniških pravic in gesel ter postopke za nadzor nad njimi,
7. dokumente, ki določajo postopke in ukrepe za upravljanje in posodabljanje ključnih sredstev (omrežij, informacijskih sistemov in naprav ter spreminjanja njihovih nastavitev),
8. dokumente, ki določajo postopke in ukrepe za odkrivanje, prepoznavanje, preiskovanje, obvladovanje, obveščanje in poročanje o varnostnih incidentih, vključno z zapisi o nastalih varnostnih incidentih in oceno njihovega vpliva na izvajanje javnih komunikacijskih storitev ter izvedenih ukrepih za njihovo preprečevanje oziroma za omilitev posledic nastanka varnostnih incidentov,
9. dokumente, ki določajo postopke, organizacijske vloge, odgovornosti in ukrepe pooblaščenih oseb za zagotavljanje neprekinjenosti poslovanja ter zahtevane ravni informacijske varnosti (varnost omrežij, informacijskih sistemov in podatkov) tudi v primeru katastrofalnega izpada ali ob naravnih in drugih nesrečah oziroma kadar je potrebno upravljanje z varnostnimi kopijami,
10. dokumente, ki določajo postopke, organizacijske vloge, odgovornosti in ukrepe pooblaščenih oseb za zagotavljanje podvojenih oziroma nadomestnih elementov omrežja in sistemov ter za vnovično vzpostavitev delovanja storitev po nepredvidenih dogodkih,
11. kadrovska politika in popis konkretnih pogojev in zahtev tudi glede usposobljenosti za zaposlene na delovnih mestih, ki so pomembna za informacijsko varnost ter nemoteno izvajanje javnih komunikacijskih storitev,
12. popis ukrepov za zagotavljanje ustrezne usposobljenosti zaposlenih, ki so odgovorni za informacijsko varnost ter za izobraževanje vseh zaposlenih na področju kibernetske varnosti,
13. dokumente, ki popisujejo zahteve, ki jih morajo izpolnjevati dobavitelji in ponudniki podpore tretje ravni (izvajanje storitev zunanjih izvajalcev pri vzpostavitvi, vzdrževanju in nadgradnjah omrežij, informacijskih sistemov ter naprav) za blažitev tveganj, povezanih z dostopi do sredstev, vključno z dogovori o zaupnosti in nerazkrivanju informacij,

14. seznam fizično varovanih komunikacijskih objektov in pasivne komunikacijske infrastrukture, ključnih za neprekinjeno delovanje storitev operaterjev ter zapise ukrepov v zvezi z varovanjem le-teh,
15. dnevnike dogodkov, ki beležijo aktivnosti, okvare in varnostne incidente na ključnih sredstvih za vsaj šest mesecev od nastanka posameznega dogodka,
16. dokumente, ki opisujejo postopke za preverjanje in ocenjevanje učinkovitosti SUVI in SUNP ter zapise o izvedenih korektivnih ukrepih.

(2) Za dokumente iz prejšnjega odstavka mora operater vzpostaviti dokumentni sistem, ki zagotavlja:
1. odobritev dokumentov, preden so objavljeni,
2. pregledovanje in dopolnjevanje dokumentov,
3. uporabo najnovejših verzij ustreznih dokumentov,
4. da bodo dokumenti na razpolago tistim, ki jih potrebujejo oziroma morajo biti z njimi seznanjeni ter
5. sledljivost in varno hrambo dokumentov.

8. člen
(varnost signalne kontrolne ravnine)

(1) Operater mora na robu omrežja in na ključnih vozliščih, kjer se izvaja izmenjava prometa (npr. HLR/HSS, MME, SMSC itd.) izvajati primerne in sorazmerne varnostne ukrepe za preprečevanje zlorab na ravni signalne kontrolne ravnine, kot je prestrezanje komunikacij in drugih podatkov, lažno predstavljanje, preprečevanje neželenih SMS sporočil, sledenje terminalom, DDoS napadi na omrežje in uporabnike.

(2) Operaterji za preprečevanje zlorab na ravni protokola SS7 v čim večji meri upoštevajo vse veljavne smernice Združenja GSMA (v nadaljevanju: GSMA) in ENISA.

9. člen
(varnost omrežij 5G)

(1) Poleg ostalih določb tega splošnega akta, operater, ki upravlja z elementi in funkcijami omrežja 5G še dodatno upošteva, da:
1. elementi in funkcije omrežja 5G izpolnjujejo funkcionalnosti in tehnične specifikacije, kot jih opredeljujejo 3GPP standardi,
2. je arhitektura in varnost omrežja 5G in njenih funkcij, izvedena v skladu z veljavnimi standardi 3GPP ter najnovejšimi priporočili ENISA in GSMA,
3. pri pripravi ukrepov upošteva ugotovljene ranljivosti, potencialne grožnje in zlonamerne akterje, kot so prepoznani v najnovejših dokumentih Skupine za NIS (»NIS Cooperation Group«), npr. Usklajena ocena tveganja za kibernetsko varnost omrežij 5G (angl. »EU Coordinated risk assessment of the cybersecurity of 5G networks, report«, oktober 2019)
4. upošteva najnovejše industrijske dobre prakse in priporočila ENISA v zvezi z varnostjo omrežij 5G (npr. »5G Supplement – to the Guideline on Security Measures under EECC«, 7. julij 2021 in »Security in 5G Specifications – Controls in 3GPP«, 24. februar 2021) ter v zvezi z virtualizacijo in virtualiziranimi omrežnimi funkcijami (npr. »NFV Security in 5G – Challanges and Best Practices«, 24. februar 2022),

5. je vzpostavljena učinkovita raven upravljanja, nadzora in varnosti omrežja 5G, še posebej pri zaznavanju nepravilnosti, zlorab in nepooblaščenih sprememb v omrežju in s strani končnih naprav,
6. ima dolgoročno strategijo raznolikosti dobavne verige in proizvajalcev opreme, ki upošteva tehnične omejitve in hkrati zagotavlja medsebojno skladnost in nemoteno delovanje,
7. izvaja logično obrambo (testiranje ranljivosti in možnih zlorab na omrežni in aplikativni ravni),
8. zagotavlja visoko raven varnosti in preprečevanja zlorab na ravni protokola mejnega prehoda (angl. »Border Gateway Protocol (BGP)«) z upoštevanjem najnovejše tehničnih usmeritev z upoštevanjem najnovejše industrijske dobre prakse (npr. Delovne skupine za internetsko inženirstvo (IETF) in ENISE oziroma drugih pristojnih institucij (npr. ENISA, »7 steps to shore up BGP«,maj 2019),
9. izvaja oceno tveganja glede dobaviteljev trajno integriranih modulov za prepoznavo in overjanje naročnikov (v nadaljnjem besedilu: eSIM/eUICC) in zagotavljanja eSIM/eUICC,
10. prednostno uporablja tiste omrežne komponente 5G ter dobavitelje varnostnih elementov in kriptografskega materiala, ki omogoča menjavo profilov in uporabo mobilnega omrežja operaterja in njegovih storitev z uporabo eSIM/eUICC, ki so prestali presojo s strani organov, akreditiranih za ugotavljanje skladnosti s posamezno evropsko certifikacijsko shemo za kibernetsko varnost, kot izhaja iz Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti).

(2) Operater pri načrtovanju ukrepov iz prejšnjega odstavka sledi dobrim praksam in splošno sprejetimi aktualnim priporočilom stroke, med drugim GSMA.

10. člen
(upravljanje tveganj v zvezi z oskrbo električne energije)

(1) Operater z distribucijskimi podjetji za oskrbo z električno energijo vzpostavi učinkovit postopek ažurnega obveščanja o vzdrževanjih in morebitnih predvidenih izpadih dobave električne energije.

(2) Na lokacijah, ki so ključna za delovanje in upravljanje omrežja in informacijskih sistemov operaterja, mora operater zagotoviti stalno neprekinjeno napajanje, ki se redno preverja in testira ob delovni obremenitvi.

(3) Operater mora imeti v času največje obremenitve vsaj dvourno avtonomijo (rezervno napajanje), ki omogoča več kot 500 naročnikom delovanje vsaj javno dostopne medosebne komunikacijske storitve na podlagi številke, SMS sporočil, javnega alarmiranja in obveščanja ter storitev komunikacij v sili, na vseh večjih dostopovnih vozliščih ter baznih postajah, ki pokrivajo naselja s statusom mesta z več kot 3 000 prebivalci.

(4) Operater mora imeti v času največje obremenitve vsaj dve urno avtonomijo (rezervno napajanje), ki omogoča več kot 250 naročnikom delovanje vsaj javno dostopne medosebne komunikacijske storitve na podlagi številke, SMS sporočil, javnega alarmiranja in obveščanja ter storitev komunikacij v sili, na vseh večjih dostopovnih

vozliščih ter baznih postajah, ki pokrivajo naselja brez statusa mesta z manj kot 3 000 prebivalci.

(5) Operater vodi popis stanja v zvezi z zagotavljanjem redundantnega napajanja.

(6) Operater sam oziroma v sodelovanju z drugimi operaterji pripravi, posodablja in izvaja načrt ukrepanja s prednostnim seznamom lokacij reševanja in obnove storitev v primeru daljšega izpada električne energije.

11. člen

(obravnava varnostnih incidentov in presoja ustreznosti ukrepov)

(1) Agencija operativno sodeluje z nacionalno skupino za obravnavanje incidentov v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: nacionalni CSIRT).

(2) Nacionalni CSIRT nudi pomoč agenciji na njeno utemeljeno zahtevo pri razreševanju in vrednotenju varnostnih incidentov in presoji sprejetih varnostnih ukrepov na strani operaterja.

(3) Agencija po potrebi lahko zaprosi za mnenje in pomoč v zvezi z izvedenimi varnostnimi ukrepi ali rešitvami na strani operaterja tudi drugo usposobljeno neodvisno inštitucijo.

12. člen
(določitev kontaktne osebe)

(1) Operater mora v organizaciji določiti kompetentno in usposobljeno osebo, ki ima pregled nad izvajanjem varnostne politike in njenega namestnika.

(2) Operater mora takoj po imenovanju osebe iz prejšnjega odstavka agenciji na njen uradni naslov oziroma uradni elektronski naslov sporočiti njegove kontaktne podatke in sicer: ime in priimek, navedbo funkcije, ki jo opravlja pri operaterju, kontaktno telefonsko številko in kontaktni elektronski naslov.

13. člen
(notranja presoja SUVI in SUNP)

(1) Operater mora najmanj enkrat letno izvesti notranjo presojo SUVI in SUNP (v nadaljnjem besedilu: notranja presoja), kjer ugotavlja učinkovitost in ustreznost sprejetih ukrepov SUVI in SUNP na podlagi zakona in tega splošnega akta. Za vsako notranjo presojo operater določi cilje, obseg in kriterije.

(2) Operater mora zagotoviti, da se v treh letih od izvedbe posamezne notranje presoje pregledajo vsi cilji ukrepov ter sprejeti oziroma posodobljeni ukrepi.

(3) Z rezultati notranjih presoj se vsakokrat seznani vodstvo. Operater mora o njih voditi zapise, ki jih hrani najmanj pet let.

(4) Operater na njeno zahtevo agenciji predloži na vpogled ali ji posreduje dokazila o izvajanju obveznosti v skladu s tem členom.

14. člen
(certificiranje)

(1) Operater, ki izvaja storitve za kritične subjekte ali ima več kot 100 000 uporabnikov, vzpostavi, izvaja, vzdržuje in nenehno izboljšuje vzdržuje SUVI in SUNP v skladu s priznanimi veljavnimi mednarodnimi standardi v obsegu, kot je določen v zakonu in tem splošnem aktu.

(2) Operater iz prejšnjega odstavka dokazuje neprekinjeno skladnost SUVI in SUNP s certifikati, ki jih izdaja akreditiran organ za ugotavljanje skladnosti. Operater mora vzdrževati in obnavljati izdane certifikate skladnosti v skladu z izbranim standardom v časovnih intervalih, kot jih določa izbrani standard.

(3) Operater na njeno zahtevo agenciji predloži na vpogled ali posreduje dokazila o izvajanju obveznosti v skladu s tem členom.

IV. PREHODNE IN KONČNA DOLOČBA

15. člen
(nov SUVI in SUNP)

Operater pripravi nov SUVI in nov SUNP skladno z zahtevami tega splošnega akta v roku enega leta od njegove uveljavitve.

16. člen
(izpolnjevanje zahtev)

(1) Operater izpolni zahteve iz prvega in drugega odstavka 14. člena tega splošnega akta v roku treh let od njegove uveljavitve.

(2) Operater, ki pisno obvesti agencijo o začetku zagotavljanja javnih komunikacijskih omrežij oziroma izvajanja javnih komunikacijskih storitev v skladu s 5. členom zakona po uveljavitvi tega splošnega akta, izpolni zahteve iz prvega in drugega odstavka 14. člena v treh letih od pisnega obvestila.

17. člen
(prenehanje uporabe)

Z dnem uveljavitve tega splošnega akta se preneha uporabljati Splošni akt o varnosti omrežij in storitev (Uradni list RS, št. 75/13, 64/15 in 130/22 – ZEKom-2).

PREDLOG!

18. člen
(začetek veljavnosti)

Ta splošni akt začne veljati trideseti dan po objavi v Uradnem listu Republike Slovenije.

Št. _____
Ljubljana, dne _____
EVA _____

mag. Mark Pohar
v.d. direktorja