Pripombe in komentarji na osnutek predloga ZInfV-1, ki ga je objavil URSIV dne 16.2.2024

15. marec 2024

Splošne pripombe na osnutek predloga ZInfV-1

Za obravnavo tako kompleksnega zakona je po našem mnenju bilo premalo časa za tehtanje določil zakona z vidika vpliva na izboljšanje kibernetske varnosti in sposobnosti podjetij na prilagajanje na zahteve zakona, kar bo imelo velik vpliv na MSP, ki jih je največ, ter tehtanju drugih potencialnih posledic zakona. Brez ustreznih ukrepov za številna MSP, ki vključujejo tudi pomoč države, se bo situacija na trgu bistveno spremenila in celo ogrozila njihovo dejavnost oz. obstoj.

Osnutek predloga ZInfV-1 gre po našem mnenju v bistveno širitev obveznosti iz NIS 2 brez ocene ustreznih posledic za gospodarstvo. Z uvajanjem dodatnih zavezancev, dodatnih obveznosti, dodatnih pristojnosti pristojnega organa in predpisovanjem dodatnih glob izven okvirov začrtanih v NIS 2, ne da bi bil narejen test sorazmernosti takšne ureditve in brez poglobljene presoje posledic za gospodarstvo, bi predlagana ureditev imela za posledico bistveno povečanje stroškov skladnosti zavezancev, kar bi oviralo razvoj takšnih subjektov, zmanjšalo obseg inovacij, negativno vplivalo na digitalno preobrazbo družb in posledično tudi zmanjšalo konkurenčnost slovenskega gospodarstva v primerjavi z drugimi državami EU, ki implementirajo varnostni okvir na sorazmeren način, brez nesorazmerne širitve kroga zavezancev in brez nalaganja dodatnih nesorazmernih bremen zavezancem.

Kot poudarja tudi združenje Digital Europe[1], ki je eno vidnejših gospodarskih združenj s področja digitalne preobrazbe v Evropi, je regulatorna usklajenost eden ključnih ciljev NIS 2 glede na predvideno širitev področja uporabe, horizontalni in sektorski pravni instrumenti pa bi morali biti dovolj usklajeni in bi se morali izogniti regulativnemu prekrivanju. Digital Europe še opozarja na pomen konsistentnega in predvidljivega poslovnega okolja in da morajo kakršnikoli ukrepi ostati sorazmerni. V tem vidiku je pomembno tudi zagotoviti, da globe ostanejo sorazmerne in upoštevajo posebnosti vsakega posameznega primera, vključno z dobro vero subjektov, na primer v primerih, ko lahko zaradi nepredvidenih okoliščin zavezanci zamudijo roke za poročanje.

[1] https://www.digitaleurope.org/resources/digitaleuropes-position-on-the-nis-2-directive/

Osnutek predloga ZInfV-1 gre po našem mnenju tudi preko strogih standardov in obveznosti, ki jih implementira NIS 2 in zaide v področje, ki je sporno z vidika sorazmernosti predlaganih ukrepov. Državam članicam bi moralo biti pri implementaciji direktive NIS 2 primarno vodilo sorazmernost v smislu posebnega področja uporabe, med drugim da se zagotovi razumnost in primernost kroga zavezancev in s tem obseg reguliranih panog in subjektov. Pojavlja se tudi dvojnost, ko bodo na primer operaterji komunikacijskih omrežij zapadli tako pod določbe o varnostnih zahtev iz ZEKom-2 kot po ZInfV-1, določbe pa niso povsem usklajene. Poseben poudarek bi bilo potrebno dati kritičnim elementom in funkcijam, razmejitev pa bi bil potrebno opredeliti na podlagi znanstvenih metod. Za izboljšanje učinkovitosti certificiranja in zmanjšanje stroškov so priporočljiva enotna merila certificiranja, širjenje obveznosti izven NIS 2 pa ni utemeljeno in zakonodajalec ne bi smel pri transpoziciji nalagati dodatnega ekonomskega bremena slovenskemu gospodarstvu. Tveganja dobavnih verig bi bilo potrebno oceniti na podlagi dejstev in standardov, zaupanje pa bi moralo temeljiti na preverljivih dejstvih, preverjanje pa bi moralo potekati po enotnih standardih.

Zakon prinaša nejasnosti glede kroga subjektov, na katere se zakon nanaša, med drugim ni pravilno implementirano načelo teritorialne pristojnosti iz 26. člena NIS 2, niso bile pravilne preslikane definicije za MSP, problematična je pristojnost vlade, da brez zakonsko določenih kriterijev oz. mimo njih določi dodatne subjekte, ki so zavezani (6. člen). Preširoke in premalo natančno definirane prisojnosti URSIV (brez ustreznih zakonskih kriterijev in zamejitev) so verjetno neskladne z Ustavo RS (npr. 8. odstavek 20. člena, ki določa blanketno pooblastilo vladi, 22. člen glede poročanja gre preko NIS 2, 4. do 8. odstavek 32. člena in 7. do 10. odstavek 33. člena določajo preširoke pristojnosti URSIV).

Obenem so nesorazmerne globe, ki ne bi smele biti zamejene navzdol (53. in 54. člen), saj NIS 2 določa zgolj zgornji prag, globe v odstotku od prometa pa bi morale biti zamejene na najhujše kršitve, kot jih predvideva 21. in 23. člen v NIS 2, širjenje kataloga kršitev pa je nesorazmerno. Obenem so preiskovalne pristojnosti URSIV preširoke in lahko pridejo v konflikt s temeljnimi ustavni in postopkovnimi varovalkami.

Osnutek predloga ZInfV-1 predvideva tudi spremembo ZEKom-2, pri čemer širi že tako nesorazmeren ukrep iz 116. člena ZEKom-2, vezan na strateške kriterije, namesto, da bi se osredotočil na objektivne in nediskriminatorne kriterije.

Pristojni nacionalni organi mora tudi jasno določiti, katere podzakonske akte je treba sprejeti za izvajanje NIS 2 direktive. To je ključno za zagotovitev dosledne implementacije in učinkovitega izvajanja ukrepov za informacijsko varnost. Pri določanju rokov za izvedbo zahtevanih ukrepov je treba upoštevati realnost ter dejstvo, da zavezanci morda nimajo vseh potrebnih informacij (navodil, tehničnih specifikacij itd.). Prilagodljivost in razumevanje teh okoliščin sta ključna za uspešno implementacijo zakona, 6 mesečni rok za prilagoditev na izvedbeni predpis pa je odločno prekratek

Dobavitelji IKT rešitev in storitev so posredno preko dobavnih verig zavezani k izvajanju ukrepov za obvladovanje tveganj informacijske varnosti prek pogodb z naročniki, zato je posebno pozornost v zakonu potrebno nameniti tudi njim. Menimo tudi, da raziskovalne organizacije ne smejo biti zavezanci po tem zakonu in naj se jih izključi.

Člani SeKV-ZIT in SRIP GoDigital KV smo pripravljeni v naslednji fazi sodelovati z URSIV pri pripravi bolj izvedljivega zakonskega predpisa, saj je naš skupen interes, da se bo zakon lahko izvajal v praksi in bo tudi administrativno kar najmanj obremenjujoč za podjetja.

S spoštovanjem,

Sekcija za kibernetsko varnost

Združenje za informatiko in telekomunikacije

SRIP GoDigital - KV

Bolj podrobne pripombe in komentarji po členih na osnutek predloga ZInfV-1 spodaj:

OPOMBA: Z rumeno barvo so označeni deli členov, katere bi bilo potrebno popraviti.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
1. člen (vsebina zakona)		
(1) Zakon ureja področje informacijske in kibernetske varnosti ter opredeljuje nacionalni sistem informacijske varnosti v Republiki Sloveniji. Pri tem ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: pristojni nacionalni organ), organa za obvladovanje incidentov velikih razsežnosti in kriz, enotne kontaktne točke za kibernetsko varnost (v nadaljnjem besedilu: enotna kontaktna točka), skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT); ureja sprejem Strategije kibernetske varnosti Republike Slovenije in določa kibernetsko obrambo ter sodelovanje pristojnih državnih organov in skupin CSIRT. (2) Ta zakon zaradi nemotenega delovanje države v vseh varnostnih razmerah ter za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji določa tudi ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznost poročanja zavezancev po tem zakonu. Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu.	(1) Na SeKV-ZIT menimo, da bi bilo potrebno besedilo 1. in 2. člena osnutka ZInfV-1 še enkrat podrobno premisliti z vidika 1. in 2. člena NIS 2 direktive. (2) Predlog zakona v 31. členu določa prostovoljno priglasitev incidentov, ki je na voljo subjektom, ki niso zavezanci po tem zakonu. V prvem odstavku je potrebno definirati, da zakon ureja tudi prostovoljno priglasitev incidentov, ki je na voljo ne-zavezancem.	
2. člen (namen zakona)		
(1) Namen zakona je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji na področjih, ki so bistvenega	Po našem mnenju bi bilo treba namen zakona dodatno opredeliti in definirati.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah. (2) S tem zakonom se v pravni red Republike Slovenije prenaša Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 333/142, z dne 27. 12. 2022, str.80), nazadnje popravljena s Popravkom Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 239 z dne 28. 9. 2023, str. 48) (v nadaljnjem besedilu: Direktiva 2022/2555).		
3. člen (področje uporabe zakona)		
(1) Ta zakon se uporablja za javne ali zasebne subjekte vrste iz Prilog I ali II tega zakona (v nadaljnjem besedilu Priloga I ali II), ki sta sestavni del tega zakona, če imajo vsaj 50 zaposlenih in letni promet ~~oziroma~~ ali letno bilančno vsoto vsaj 10 milijonov evrov.	SeKV-ZIT meni, da bi bilo potrebno 3. člen uskladiti s prvim odstavkom 26. člena NIS 2 direktive, tako da se v 3. člen (ali na drugem ustreznem mestu) doda teritorialna pristojnost (za vso materijo ZInfV-1), kakor jo določa NIS 2:	Teritorialna pristojnost je urejena zgolj parcialno v 27. členu, in sicer vezano na pristojnost skupine CSIRT, ki ji zavezanci priglašajo incidente. Ni pa teritorialna pristojnost splošno urejena v zakonu v skladu z NIS 2.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
(2) Ta zakon se uporablja za subjekte iz prejšnjega odstavka ne glede na njihovo število zaposlenih ali letni promet oziroma letno bilančno vsoto, kadar: - 1. storitev opravljajo: - ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, - ponudniki storitev zaupanja, - registri vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen; - 2. je subjekt edini ponudnik storitve, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti v Republiki Sloveniji; - 3. bi motnja pri opravljanju storitve subjekta lahko pomembno vplivala na javni red, javno varnost ali javno zdravje; - 4. bi motnja pri opravljanju storitve subjekta lahko povzročila pomembno sistemsko tveganje, zlasti za sektorje, v katerih bi lahko taka motnja imela čezmejni vpliv; - 5. je subjekt kritičen zaradi njegovega posebnega pomena na državni, regionalni ali lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v Republiki Sloveniji;	*»Subjekti na podlagi te direktive spadajo v pristojnost države članice, kjer imajo sedež, razen v primeru, da:* *-se za ponudnike javnih elektronskih komunikacijskih omrežij ali ponudnike javno dostopnih elektronskih komunikacijskih storitev šteje, da spadajo v pristojnost države članice, v kateri zagotavljajo svoje storitve;* *-se za ponudnike storitev DNS, registre TLD imen, subjekte, ki opravljajo storitve registracije domenskih imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov, ponudnike omrežij za dostavo vsebine, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev ter ponudnike spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja šteje, da spadajo v pristojnost države članice, v kateri imajo glavni sedež v Uniji v skladu z odstavkom 2;«* (1) Pri osnutku je prišlo do redakcijske napake pri prenosu kriterijev za srednje veliko družbo, ki predlagamo, da se odpravi. Prvi odstavek bi bilo potrebno spremeniti tako, da se beseda »oziroma« nadomesti z »ali«, tako da je razvidno, da morata biti izpolnjena dva od treh kriterijev.	Povsem nesorazmerna bi bila obveznost, da bi preostale določbe zakona (v nasprotju z NIS 2 direktivo) imele univerzalno veljavnost (vključno z obveznostjo samoregistracije po 7. členu) in bodo veljale za vse subjekte po celem svetu, tudi takšne, ki nimajo povezave z Republiko Slovenijo (in ne izvajajo storitev v RS in v njej nimajo sedeža). Navedeno predstavlja tudi tveganje za multinacionalke in za pravne osebe s sedežem v Sloveniji, da bi tudi vse njihove povezane osebe (npr. sestrske družbe in nadrejene družbe) morale izvajati samoregistracijo v Republiki Sloveniji v nasprotju z namenom NIS 2. Navedeno tudi ruši koncept NIS 2 glede registracije po posameznih državah, saj bi se bile družbe zavezane samoregistrirati tudi v Republiki Sloveniji (poleg registracije v relevantni pristojni državi EU). (1) NIS 2 določa, da se direktiva uporablja za javne ali zasebne subjekte vrste iz Priloge I ali II, ki izpolnjujejo pogoje za srednja podjetja iz člena 2 Priloge k Priporočilu 2003/361/ES, ali presegajo zgornje meje za srednja podjetja. Skladno z drugim odstavkom navedenega priporočila velja: "Within the SME category, a small enterprise is defined as an enterprise

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
- 6. gre za subjekt javne uprave na državni ravni ali na regionalni ravni in - 7. gre za subjekt javne uprave na lokalni ravni, če pri slednjem izhaja iz njegove ocene tveganja, da opravlja storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti. (3) Ta zakon se uporablja tudi za subjekte, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo. (9) Kadar področni predpisi zahtevajo, da subjekti, ki so bistveni ali pomembni subjekti po tem zakonu, sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost oziroma da priglasijo pomembne incidente, in kadar so takšne zahteve področnih predpisov po učinku vsaj enakovredne obveznostim iz tega zakona, se ustrezne določbe tega zakona, vključno z določbami o nadzoru iz poglavja IX in kazenskimi določbami iz poglavja X, za take subjekte ne uporabljajo. Kadar področni predpisi ne zajemajo vseh subjektov v določenem sektorju iz Priloge I ali II, ki spadajo na področje uporabe tega zakona, se ustrezne določbe tega zakona še naprej uporabljajo za subjekte, ki niso zajeti v takšnih področnih predpisih.	(3) Potrebno je bolj natančno definirati na kateri zakon o kritični infrastrukturi se to nanaša. (9) SeKV-ZIT zanima, kdo in kako oz. kje bo določil, kateri področni predpisi bodo določali enakovredne ukrepe za obvladovanje oz. priglasitev incidentov? Potrebno je določiti bistvene in pomembne subjekte iz prilog I in II. Predlagamo tudi brisanje 7. točke drugega odstavka in šestega odstavka, ki gresta preko dometa NIS 2. NIS 2 ne določa obveznosti uporabe za subjekte javne uprave na lokalni ravni, vendar peti odstavek 2. člena NIS 2 dopušča, da lahko države članice odločijo, da se direktiva uporablja tudi za le-te. Glede na to, da pravo EU ne zahteva, da bi se moral ZInfV-1 uporabljati tudi za te subjekte, bi bilo v zvezi z navedeno razširitvijo uporabe NIS 2 potrebno izvesti tudi presojo posledic in upoštevati načelo sorazmernosti. Ne zdi se skladno z načelom enakosti, da bi se ZInfV-1 uporabljal za vse občine (subjekte lokalne samouprave) in subjekte javne uprave na lokalni ravni, saj gre NIS 2 v smeri varstva subjektov javne uprave na osrednji državni ravni ter subjektov javne uprave na regionalni ravni (npr. organih posameznih zveznih držav v zveznih državah, npr. Avstriji, Nemčiji). Takšna omejitev	which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million."

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
	ima seveda potencialno tudi vpliv na gospodarstvo in svobodo gospodarske pobude, če bo širši krog zavezancev zapadel pod omejitve glede dobavnih verig, zaradi česar bi moral biti opravljen test sorazmernosti.	
4. člen (obdelava podatkov in informacij)		
(1) Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev pa tudi v skladu s predpisom, ki ureja zasebnost na področju elektronskih komunikacij. Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij pomeni zakoniti interes zadevnega upravljavca podatkov. (2) Podatki in informacije, ki se obdelujejo na podlagi tega zakona in so opredeljeni kot tajni ali kot poslovna skrivnost ali druge oblike varovanih podatkov, se obravnavajo v skladu s področnimi predpisi, ki urejajo njihovo obravnavo in varovanje. zmenjava podatkov in informacij, ki so opredeljeni kot tajni ali poslovna skrivnost mora biti za potrebe izvajanja tega zakona omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij ter zaščiti varnost in poslovni interes zadevnih subjektov.	(1) SeKV-ZIT je mnenja, da je to ustrezno opredeljeno v ZVOP oziroma GDPR (uvodna določba GDPR 49). Ob enem nas zanima, kako to določbo umestiti v kontekst zahtev člena 6(1)(f) GDPR, predvsem zahteve po izdelavi LIA? (2) Določbe 2. in 5. odstavka, ki se nanašajo na tajne podatke, ki jim je stopnja tajnosti določena po ZTP, je treba uskladiti z ZTP. (5) Ti podatki so oz. bi morali biti določeni, označeni in varovani kot tajni podatki po ZTP (5.,11. in 13. člen)	Utemeljitev SeKV-ZIT: Če so to podatki, ki so določeni za bančno, davčno, statistično,...tajnost, kot izhaja iz obrazložitve predloga zakona, se bi bilo vseeno treba vprašati, kje bodo meje izmenjave tovrstnih podatkov in kdo/kako bo reševal morebitni konflikt med zavezancem in organom, ki dotične informacije zahteva. Izjema po ZDIJZ bi morala biti vključena v 6. člen omenjenega zakona. Potrebna je tudi vključitev ZTP v ta zakon

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
(3) Izmenjava podatkov in informacij, ki so varovani podatek pristojnega nacionalnega organa, mora biti za potrebe izvajanja tega zakona omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij ter zaščiti varnost in poslovni interes zadevnih subjektov. Ne glede na določbe zakona, ki ureja dostop do informacij javnega značaja, se varovani podatki pristojnega nacionalnega organa ne posredujejo javnosti. (5) Obveznost izmenjave podatkov na podlagi tega zakona ne vključujejo posredovanja podatkov in informacij, katerih razkritje bi bilo v nasprotju z vitalnimi interesi Republike Slovenije na področju nacionalne varnosti, javne varnosti ali obrambe, izven Republike Slovenije.		
5. člen (pomen izrazov)		
Izrazi, uporabljeni v tem zakonu, imajo naslednji pomen: 7. Incident pomeni dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih ti omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni. 13. Kibernetska higiena pomeni dobro prakso ohranjanja varnosti in zaščite informacij v	(7) SeKV-ZIT predlaga, da bi bilo potrebno upoštevati tudi definicijo incidenta iz DORA: „incident, povezan z IKT“ pomeni enkraten dogodek ali vrsto povezanih dogodkov, ki jih finančni subjekt ni predvidel ter ki ogrožajo varnost omrežnih in informacijskih sistemov in škodljivo vplivajo na razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov ali na storitve, ki jih opravlja finančni subjekt	Zakon nalaga izključna pooblastila in naloge pregledovanja informacijskih sistemov preizkušenim revizorjem informacijskih sistemov, ki so registrirani pri Slovenskem inštitutu za revizijo in vpisani v njegov seznam aktivnih preizkušenih revizorjev informacijskih sistemov. Glede na namen zakona je takšna določba preozka in glede na pričakovan obseg zavezancev ter števila revizorjev, zato predlagamo vključitev vseh revizorjev,

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
digitalnem okolju. To vključuje različne ukrepe in postopke, namenjene zaščiti računalniških sistemov, omrežij ter podatkov pred različnimi varnostnimi grožnjami. 39. Preizkušeni revizor pomeni preizkušenega revizorja informacijskih sistemov, ki je registriran pri Slovenskem inštitutu za revizijo in vpisan v njegov seznam aktivnih preizkušenih revizorjev informacijskih sistemov. 40. Proizvod IKT pomeni element ali skupino elementov omrežja ali informacijskega sistema. 45. Revizijska sled je nespremenljiva sled oziroma niz podatkov o dogodku, ki se je zgodil v informacijskem sistemu ali napravi, z natančnim časovnim zapisom v obliki dnevniškega zapisa, ki omogoča natančen pregled vseh zapisov, povezanih z vsemi dogodki in vsemi shranjenimi informacijami, od nastanka podatka ali informacije naprej do trenutnega stanja. 65. Varovan podatek pristojnega nacionalnega organa je podatek o ranljivostih ali stanju informacijskih sistemov in omrežij zavezancev, ki ni tajen ali poslovna skrivnost njegovo razkritje nepoklicanim osebam pa bi lahko povzročilo motnje pri delovanju in izvajanju nalog pristojnemu nacionalnemu organu, oziroma bi lahko škodovalo zavezancem.	(13) Izraz je potrebno jasno definirati, tako da bo jasno kaj se od zavezancev zahteva. Ne kako tehnično izvesti, vendar katera področja je potrebno pokriti. Lahko se sklicuje na mednarodne standarde. (39) Definicija pojma naj se uskladi z definicijo pojma v Zakonu o revidiranju. SeKV-ZIT predlaga prehodno obdobje, da bi se usposobilo več revizorjev za izvedbo ali pa vključitev dodatnih revizorjev ISO 27001 v izvajanje revizije. (40) Namesto besede proizvod, predlagamo uporabo besede sredstvo (57) Potrebna je uskladitev definicije v skladu z eIDAS 2. (65) Zanima nas, kdo bo ta podatek določil in kako ga bo označil?	ki so v javnem registru PRIS, katerih naj bi bilo več kot 100 strokovnjakov z licenco, ki lahko v rokih, ki jih zakonodajalec nalaga zavezancem, izpolnijo pogoje za izvajanje tovrstnih revizij. Poleg tega v celoti spregleda številne mednarodno priznane standarde s področja informacijske varnosti in neprekinjenega poslovanja, kjer strokovnjaki z ustreznim certifikatom presojevalca in strokovnimi izkušnjami, ki jih preverjajo mednarodne akreditacijske hiše, v najmanj enaki meri izpolnjujejo kriterije za izvajanje tovrstnih presoj. Dodaten pomislek k takšni opredelitvi izvira iz samega namena direktive NIS 2, ki želi razširiti področje varovanja informacij na poslovodenje, procese, dobavne verige in se ne osredotoča zgolj na zagotavljanje varovanja informacijsko komunikacijskih sistemov.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
6. člen (zavezanci)		
(1) Subjekti, ki spadajo v področje uporabe tega zakona po 3. členu tega zakona, so zavezanci po tem zakonu in se delijo na bistvene in pomembne subjekte. (2) Za namene tega zakona se šteje, da so bistveni subjekti: 1.subjekti vrste iz Priloge I, ki imajo vsaj 250 zaposlenih in letni promet vsaj 50 milijonov evrov ~~oziroma~~ ali letno bilančno vsoto vsaj 42 milijonov evrov; 2. ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost; 3. ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov; 4. subjekti javne uprave na državni ravni; 5. vsi drugi subjekti vrste iz Prilog I ali II, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada z odločbo; 6. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo; 7. subjekti, ki so bili v skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 –	Glejte naš predlog, k 3. členu, ki se smiselno nanaša tudi na 6. člen. (2) V prvi točki drugega odstavka bi bilo potrebno besedo »oziroma« nadomestiti z »ali«. (2) SeKV-ZIT ne vidi razloga, da vsi kriteriji za določitev zavezancev ne bi bilo določeni v samem zakonu in da je dopuščeno Vladi RS, da sama (brez vnaprej zakonsko določenih kriterijev) določi dodatne zavezance (peta točka in osma točka drugega odstavka). Predlagamo, da se navedeno črta, takšno blanketno pooblastilo pa bi bilo tudi v nasprotju s 120. členom Ustave in 87. členom Ustave. (4) Potrebno je brisati besedico »lahko«.	Utemeljitev: Po našem mnenju drugi odstavek šestega člena ni v skladu z razmejitvijo iz NIS 2. NIS 2 se sklicuje na subjekte vrste iz Priloge I, ki presegajo zgornje meje za srednja podjetja, določene v členu 2(1) Priloge k Priporočilu 2003/361/ES. Relevantna določba določa "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million."

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
ZDU-1O in 49/23) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023; 8. drugi subjekti, ki niso subjekti iz točk 1 do 7 tega odstavka, ki jih vlada lahko določi kot bistvene subjekte zaradi pomembnega negativnega vpliva, ki bi ga incident pri izvajanju njihovih storitev imel za življenje in zdravje ljudi oziroma zaradi pomembnega negativnega vpliva na okolje. (4) Izvajanje 8. točke drugega odstavka tega člena vlada ~~lahko~~ podrobneje opredeli z metodologijo za določitev zadevnih subjektov kot bistvenih.		
7. člen (samoregistracija in seznam zavezancev)		
(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz prejšnjega člena tega zakona. (2) Zavezanci iz prejšnjega člena tega zakona se morajo registrirati preko mehanizma za samoregistracijo iz prejšnjega odstavka in ob tem podati vsaj naslednje informacije o: - imenu in naslovu, kontaktnih podatkih, matični številki ter elektronskem naslovu zavezanca za vročanje; - dodeljenih blokih javnih naslovov IP; - kontaktni osebi za informacijsko varnost in njenem namestniku ter njune kontaktne podatke vključno z elektronskimi naslovi in telefonskimi številkami;	SeKV-ZIT zagovarja, da naj bi tudi novi zakon ohranil sedanji način določanja in evidentiranja bistvenih in pomembnih subjektov (zavezancev) z odločbo pristojnega državnega organa (URSIV). Omenjen je bi tudi novi hrvaški zakon o kibernetski varnosti, ki je uzakonil neke vrste hibridno rešitev. Pristojni državni organi zavezance identificirajo, razvrstijo in evidentirajo z uporabo podatkov relevantnih uradnih evidenc in registrov in podatkov, ki jih na poziv ali samoiniciativno (ob morebitnih spremembah, ki so predmet evidentiranja) posredujejo zavezanci. Tak pristop bi bil možen tudi pri nas, bil bi bolj racionalen, celovit in natančen kot	Predlog člena prenaša določbe tretjega, četrtega in petega odstavka 3. člena Direktive 2022/2555 (NIS 2). Te določbe direktive v tretjem odstavku določajo dolžnost držav članic, da oblikujejo seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen in ga redno (vsaj vsaki dve leti) pregledajo in po potrebi posodijo. Vzpostavitev mehanizma za samoregistracijo ni obveznost, ampak ena od možnosti. 4. pododstavek četrtega pododstavka 3. člena NIS2: *Države članice **lahko** vzpostavijo nacionalne mehanizme za samoregistracijo subjektov.*

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
- ustreznem sektorju in podsektorju iz Priloge I ali II, v katerem zavezanec izvaja vrste storitev iz teh prilog ali kategorijo zavezancev, ki niso vključeni v navedenih prilogah, so pa zavezanci na podlagi določb tretjega do sedmega odstavka 3. člena tega; - seznamu držav članic Evropske unije, kjer opravljajo storitve, ki spadajo na področje uporabe tega zakona ter - registriranih številkah avtonomnih sistemov in vseh domenskih imenih, ki jih zavezanec uporablja pri poslovanju." (3) Zavezanci iz prejšnjega člena tega zakona z uporabo mehanizma za samoregistracijo nemudoma sporočijo morebitne spremembe podatkov, ki so jih predložili na podlagi prejšnjega odstavka, v vsakem primeru pa v dveh tednih od datuma spremembe. (4) Na podlagi informacij zavezancev iz drugega in tretjega odstavka tega člena in ob upoštevanju določb drugega, tretjega oziroma četrtega odstavka prejšnjega člena tega zakona pristojni nacionalni organ vzpostavi seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Ta seznam pristojni nacionalni organ redno oziroma vsaj vsaki dve leti pregleda in po potrebi posodobi. (9) Organi, ki so pristojni za izvajanje področnih predpisov iz devetega odstavka 3. člena tega zakona,	predlagana rešitev. Ob tem ni odveč omeniti, da vzpostavitev seznama zavezancev ni neka enkratna aktivnost, prav tako pa seznam ne bi smel biti namenjen samo preštevanju bistvenih in posebnih subjektov, ampak bi moral biti del celovitega informacijskega sistema pristojnega nacionalnega organa in drugih pooblaščenih organov, ki bi - neposredno ali posredno - obsegal vse dogodke, povezane s področjem informacijske varnosti (priglašeni incidenti, izvedeni inšpekcijski nadzori, udeležba na usposabljanjih, vajah, pogodbeni zunanji izvajalci...). (4) Ta seznam, ki ga bo vodil URSIV, bo informacija javnega značaja. Zanima nas ali bo objavljen, ali bo dostopen na zahtevo, ali bo dostop omejen? Če bo omejen, ali bo izjema po 6. členu ZDIJZ, in če da, katera izjema bo?	NIS 2 v uvodni izjavi 18 v zadnjem stavku izrecno omenja: *Če obstajajo registri na nacionalni ravni, se lahko države članice odločijo o ustreznih mehanizmih, ki omogočajo identifikacijo subjektov, ki spadajo na področje uporabe te direktive.* Po naše mnenju lahko URSIV za lastne potrebe že izdelal nek informativni, neizključen seznam zavezancev. Možen bi bil nek hibridni način oblikovanja seznama, ki bi obsegal izhodiščno evidentiranje zavezancev na podlagi uradnih evidenc (npr. Poslovnega registra AJPES-a, Registra proračunskih uporabnikov pri Upravi za javna plačila) in potrditev ter dopolnitev (doregistracijo) evidentiranih podatkov s strani zavezancev. Glede na to, da je seznam bistvenih in pomembnih subjektov neizogibno dejstvo, bi URSIV identificirane zavezance lahko že informativno obvestil o njihovem statusu in obveznostih.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
v 30 dneh od uveljavitve takšnega področnega predpisa seznanijo pristojni nacionalni organ z identiteto subjektov (ime in naslov) s področja njihove pristojnosti, ki so na podlagi prej navedene določbe izključeni s področja uporabe zadevnih določb tega zakona ter o izpolnjevanju pogojev za takšno izključitev iz desetega odstavka 3. člena tega zakona. Pristojni nacionalni organ z organi pristojnimi za izvajanje takšnih področnih predpisov sodeluje na podlagi 5. točke 9. člena in 17. člena tega zakona.		
9. člen (pristojni nacionalni organ)		
(1) Pristojni nacionalni organ je Urad Vlade Republike Slovenije za informacijsko varnost. (2) Pristojni nacionalni organ poleg drugih nalog, določenih s tem zakonom, izvaja še naslednje naloge: 7. koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za dvig zavedanja javnosti o informacijski varnosti, lahko pa tudi sam organizira in izvaja usposabljanja s področja informacijske in kibernetske varnosti; 22. izvaja naloge nacionalnega certifikacijskega organa za kibernetsko varnost; (3) Pristojni nacionalni organ o njegovi določitvi ter nalogah in vsakokratnih spremembah pri tem brez nepotrebnega odlašanja uradno obvesti Evropsko komisijo.	(2) 7. točka: Menimo, da bi to morali postaviti v kontekst zahteve po usposabljanju odgovornih oseb in osebja zavezancev iz 19. člena predmetnega zakona. (2) 22 točka: SeKV-ZIT predlaga, da naj bo certifikacijski organ imenovan po Zakonu o akreditaciji ZAkr (ENISA določa certifikacijski postopek na ravni EU)	Certifikacijski organ bi morala določiti Slovenska akreditacija, in sicer v skladu z Zakonom o slovenski akreditaciji, Uredbo (EU) 2019/881 in členom 24 NIS 2 direktive, ki vzpodbuja ("zlasti") uporabo proizvodov, storitev in postopkov IKT, ki so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi člena 49 Uredbo (EU) 2019/881. Člen 25 NIS 2 direktive določa tudi, da naj države članice spodbujajo uporabo evropskih in mednarodnih standardov in tehničnih specifikacij, pomembnih za varnost omrežnih in informacijskih sistemov.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
15. člen (sodelovanje skupin CSIRT z deležniki zasebnega sektorja)		
(1) Skupini CSIRT iz prvega odstavka 12. člena tega zakona za dosego ciljev tega zakona vzpostavita sodelovanje z ustreznimi deležniki iz zasebnega sektorja. (2) Za olajšanje sodelovanja iz prejšnjega odstavka skupini CSIRT spodbujata sprejetje in uporabo skupnih ali uveljavljenih praks, sistemov razvrščanja in taksonomij v zvezi s: - postopki obvladovanja incidentov; - obvladovanjem kriz ter - usklajenim razkrivanjem ranljivosti na podlagi prvega odstavka 16. člena tega zakona. (3) Skupina CSIRT, ki zazna ranljivost informacijsko-komunikacijskega sistema, mora o tem brez nepotrebnega odlašanja obvestiti skrbnika sistema.	(3) Kdo je "skrbnik sistema"? Ta izraz se pojavlja še v 19. členu. SeKV-ZIT meni, da ga je potrebno definirati v 5. členu (pomen izrazov) 7. člen predmetnega zakona kot enega od podatkov seznama bistvenih in pomembnih subjektov določa kontaktno osebo za informacijsko varnost in njenega namestnika. Ali je to enako kot skrbnik sistema?	
19. člen (upravljanje)		
(3) Odgovorne osebe iz prvega odstavka tega člena se morajo izobraževati oziroma usposabljati na področju obvladovanja tveganj kibernetske varnosti in njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt. (4) Odgovorne osebe zagotavljajo redno usposabljanje zaposlenim, da pridobijo dovolj znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt.	(3) SeKV-ZIT zanima ali bodo vsebina, obseg in način usposabljanj še kakorkoli dodatno opredeljeni? In kdo bo izvajal usposabljanja za trenerje? Bo URSIV tisti, ki bo vzpostavljal ali imenoval tiste, ki bodo usposabljali. (4) Zahtevo po "rednem usposabljanju" je potrebno bolj natančno definirati. Potrebno je določiti, kateri profil zaposlenih se mora usposabljati vsako leto in kaj je vsebina	Utemeljitev: Menimo, da je potrebno natančneje opredeliti to zahtevo v izvedbenih aktih. Bilo bi smiselno, da pristojni organ poda neka priporočila (generični nabor groženj, predlog metodologij ocenjevanja tveganj, ki se uporabi, če subjekt nima že sprejete metodologije? Ali je smiselno razmisliti tudi o oceni vpliva na poslovanje?

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
(5) Ne glede na prejšnji odstavek odgovorne osebe zagotavljajo, da imajo vsi skrbniki informacijsko komunikacijskih sistemov zavezanca obveznost rednega letnega usposabljanja, da pridobijo in ohranijo raven znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt.	tega usposabljanja, t.j. ocenjevanje in obvladovanje tveganj.	
20. člen **(ukrepi za obvladovanje tveganj za KV bistvenih in pomembnih subjektov)**		
(3) Ukrepi iz prvega in drugega odstavka tega člena morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščititi omrežne in informacijske sisteme ter njihovo fizično okolje pred incidenti, in morajo obsegati najmanj: politike o analizi tveganja in varnosti informacijskih sistemov; obvladovanje incidentov; neprekinjeno poslovanje, vključno z upravljanjem varnostnih kopij in vnovično vzpostavitvijo delovanja po nepredvidljivih dogodkih ter za obvladovanje kriz; varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev; varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti; politike in postopke za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost; osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;	(3) SeKV-ZIT predlaga, da se zgledujemo po določbi 12. člena veljavnega ZinfV, saj je odlično napisan: -prvi odstavek: Izvajalci bistvenih storitev za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja... -tretji odstavek: Vlada podrobneje določi vsebino in strukturo varnostne dokumentacije iz prvega odstavka tega člena. (4) SeKV-ZIT predlaga, da se v četrtem odstavku besedilo »rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih lahko pripravi Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA« nadomesti z »rezultate	Utemeljitev: Četrti odstavek je bistveno manj določen kot tretji odstavek 21. člena NIS 2, ki naj bi se implementiral s to določbo. V NIS 2 je razvidno, da se določba nanaša na konkretne ocene tveganj, ki bodo izvedene na podlagi 22. člena NIS 2 in ne kar splošno. Tako se predlog odmika od NIS 2 in predlagamo, da se neskladje popravi. Utemeljitev za (8): Skladno z drugim odstavkom 120. člena Ustave upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov (legalitetno načelo), kar vključuje tudi zahtevo po vsebinski vezanosti uprave na ustavo in zakon, ki zagotavlja, da se posamezniki in

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem; varnost človeških virov, politike nadzora dostopa in upravljanje sredstev; uporaba večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je to primerno. (4) Bistveni in pomembni subjekti pri preučevanju ustreznih ukrepov iz 4. točke prejšnjega odstavka, morajo upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Bistveni in pomembni subjekti morajo ugotavljati tudi kateri ukrepi so ustrezni za zagotovitev varnosti dobavne verige iz 4. točke prejšnjega odstavka. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih lahko pripravi Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA. (6) Ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja in ponudniki storitev	morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki bodo izvedene v skladu s členom 22(1).Direktive 2022/2555.« Predlagamo, da se črta predlagani osmi odstavek, ker gre za blanketno pooblastilo, ki bi bilo v nasprotju s 120. členom Ustave RS: K zakonu je potrebno predložiti tudi osnutek uredbe o izvajanju ukrepov ZinfV-1 (kot je obstoječa uredba). (7) Za zgled se lahko vzame ureditev iz DORA in na njeni podlagi izdani RTS ter eIDAS 2 in na njeni podlagi izdani izvedbeni akti. (8) V zvezi z osmim odstavkom SeKV-ZIT predlaga črtanje, ker bi bilo tako široko blanketno pooblastilo verjetno v nasprotju z ustavo in problematično v praksi.	pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali. Skladno s 87. členom Ustave pa lahko pravice in obveznosti državljanov ter drugih oseb državni zbor določa le z zakonom, kar predstavlja tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon. Predlagatelj je urejanje materije iz osmega odstavka v celoti prepustil podzakonskemu predpisu Vlade, kar je v nasprotju z ustavnim načelom legalitete, še posebej ker lahko omejitve glede dobavnih verig posegajo na trg (torej tudi na prosto nastopanje dobaviteljev na trgu) in s tem omejitev ali določitev načina uresničevanja svobodne gospodarske pobude (74. člen Ustave RS). Navedene problematike po vsebini ne reši dikcija, da naj bi vlada določala zgolj »način izvajanja obveznosti« in »varnostne ukrepe«, saj je vsebina 20. člena zelo splošna (na nivoju smernic, ki splošno govorijo o

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
zaupanja pri sprejemu ukrepov iz tretjega odstavka tega člena upoštevajo izvedbene akte Evropske komisije iz prvega pododstavka petega odstavka 21. člena Direktive 2022/2555, s katerimi ta določi tehnične in metodološke zahteve za ukrepe. (7) Bistveni in pomembni subjekti, ki niso navedeni v prejšnjem odstavku, pri sprejemu ukrepov iz tretjega odstavka tega člena, upoštevajo morebitne izvedbene akte Evropske komisije, s katerimi ta določi tehnične in metodološke zahteve ter po potrebi sektorske zahteve za ukrepe iz drugega pododstavka petega odstavka 21. člena Direktive 2022/2555. (8) Vlada lahko podrobneje določi način izvajanja obveznosti iz tega člena in minimalni obseg varnostnih ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, v kolikor niso zajeti v dokumentih Evropske komisije iz šestega ali prejšnjega odstavka tega člena. Pri tem vlada upošteva tudi morebitne dokumente ali tehnična priporočila ENISA ter Skupine za sodelovanje.		obveznosti sprejeti ustrezne ukrepe) in nekonkretizirana. Predpisovanje načina izvajanja obveznosti sprejeti ustrezne ukrepe, pa bi bilo dejansko originarno predpisovanje ukrepov in bi obenem predstavljalo določitev načina uresničevanja svobodne gospodarske pobude, kar bi še vedno morala biti zakonska materija. Glede na odprtost in splošnost 20. člena preprosto ni mogoče šteti, da bi vlada s podzakonskim predpisom sploh lahko podrobneje urejala zakonsko materijo in pri tem sledila namenu in ciljem zakona.
21. člen (dnevniški zapisi)		
(1) Bistveni in pomembni subjekti za namen obvladovanja in preprečevanja incidentov, v skladu s politikami o analizi tveganja in varnosti informacijskih sistemov iz prve točke tretjega odstavka 20. člena tega zakona in ob upoštevanju stanja tehnike zagotovijo tudi ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih	SeKV-ZIT meni, da ima omejitev hranjenja dnevniških zapisov na izključno Republiko Slovenijo neblagodejen in v skrajnih primerih tudi zaviralen učinek na zasnovo kibernetske obrambe zavezancev po Zakonu, zato predlagamo spremembo drugega odstavka.	Dodatno: Če dnevniški zapisi vsebujejo osebne podatke, mora subjekt preveriti, ali mora upoštevati zahteve iz 22. člena ZVOP-2 (vodenje dnevnika obdelave). Namen hrambe dnevniških zapisov iz prvega odstavka predmetnega člena -

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
informacijskih sistemov ali delov omrežja, 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. (2) Ohranjanje dnevniških zapisov se zagotavlja na ozemlju ~~Republike Slovenije, razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, glede katerih se lahko zagotavlja na ozemlju~~ Evropske unije.	Večina osrednjih proizvajalcev (ti zmogljivosti svojih rešitev na letni ravni ocenjujejo po kriterijih industrijskega ogrodja MITRE Engenuity) namreč ponuja varnostne rešitve v oblaku, ki z vidika zmogljivosti razpoložljivosti in kibernetske odpornosti prinašajo številne prednosti. NIS 2 direktiva ne vsebuje nobene zahteve, kje naj se dnevniški zapisi hranijo, temveč le: "Države članice se tudi spodbuja, naj mikro podjetjem in malim podjetjem, ki nimajo teh zmogljivosti, ponudijo storitve, kot sta konfiguracija spletišč in omogočanje beleženja." SeKV-ZIT meni, da naj bo vse dnevniške zapise dovoljeno hraniti vsaj na območju EU.	obvladovanje in preprečevanje incidentov - se ujema z namenom vodenja dnevnika obdelave iz prvega odstavka 22. člena ZVOP-2: "...kadar je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave". ZVOP-2 določa daljše roke hrambe podatkov dnevnika obdelave; 2 oz. 5 let
22. člen (obveza posredovanja podatkov in informacij)		
(1) Bistveni in pomembni subjekti morajo pristojnemu nacionalnemu organi na podlagi pisne zahteve posredovati podatke in informacije brez nepotrebnega odlašanja, ki jih pristojni nacionalni organ potrebuje za izvajanje svojih pristojnosti po tem zakonu. (2) Zahtevani podatki in informacije morajo biti sorazmerni namenu, za katerega bodo uporabljeni. Pristojni nacionalni organ mora v zahtevi navesti namen uporabe zahtevanih podatkov in informacij.	Menimo, da je 22. člen presplošen in gre preko obsega NIS 2. Predlagamo, da se inšpekcijske / nadzorstvene pristojnosti omejijo na pristojnosti, ki jih predvideva NIS 2 (ki so že rezultat tehtanja med drugim tudi z vidika sorazmernosti in procesnih jamstev). V nasprotnem (ko gre za dodatno širjenje pristojnosti) verjetno ne bo podana sorazmernost in je ureditev problematična z vidika ustavnih jamstev. Navedeno velja splošno tudi za preostale določbe glede nadzora in inšpekcijskih pristojnosti. Posredovanje informacij (z ustrezno zamejitvijo oz. predpostavkami) je že urejeno v 5. točki drugega	Utemeljitev: Ne gre le ta uporabo kvalificiranih storitev zaupanja pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, ampak za uporabo kvalificiranih storitev zaupanja pri izvajanju procesov za zagotavljanje bistvenih oz. pomembnih storitev.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
	odstavka 41. člena predloga (v smislu točke (d) drugega odstavka 33. člena NIS 2).	
23. člen (certifikacijske sheme KV)		
(1) Bistveni in pomembni subjekti zaradi zagotavljanja višje ravni kibernetske varnosti z namenom zagotovitve skladnosti z nekaterimi zahtevami iz 20. člena tega zakona prednostno uporabljajo proizvode IKT, storitve IKT in postopke IKT ter so jih razvili bistveni ali pomembni subjekti ali ki so bili kupljeni pri tretjih straneh in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi člena 49 Uredbe (EU) 2019/881. (2) Pristojni nacionalni organ spodbuja bistvene in pomembne subjekte, da pri izvajanju ~~ukrepov iz 20. člena tega zakona~~svojih storitev, kjer je to možno in primerno, uporabljajo kvalificirane storitve zaupanja.	(2) Zanima nas kako oz. s katerimi ukrepi namerava URSIV bistvene in pomembne subjekte spodbujati k večji/pogostejši uporabi kvalificiranih storitev zaupanja? Morda bi kazalo omeniti, da gre za storitve, ki jih določa in ureja eIDAS. V nasprotnem primeru predlagamo, da se brišejo: »*ukrepi iz 20. Člena tega zakona*«. 23. člen tudi ni povsem usklajen s členom 24 NIS 2. 24. člen NIS 2 ne predpisuje obveznosti uporabe certifikacijskih shem, dopušča pa možnost, da država članica to predpiše za konkretne točno določene (angleško »particular«) ICT produkte, storitve ali procese, npr. tiste, ki so posebno kritični. V 23. členu je izpadla vsebinska zamejitev (na npr. kritične elemente) in bi bilo potrebno določbo spremeniti / prilagoditi v duhu NIS 2. Glejte angleško verzijo direktive (slovenski prevod Direktive je potrebno razumeti tudi v kontekstu angleške verzije): *»In order to demonstrate compliance with particular requirements of Article 21, Member States **may** require essential and important entities to use **particular** ICT products, ICT services and ICT processes … that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.«*	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
24. člen (standardizacija)		
(1) Bistveni in pomembni subjekti zaradi zagotovitve skladnega izvajanja ukrepov iz 20. člena tega zakona v čim večji meri uporabljajo evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov. Pri tem upoštevajo tudi nasvete in smernice ENISA. (2) Pristojni nacionalni organ na svoji spletni strani objavlja ustrezne informacije iz prejšnjega odstavka ter osvešča zavezance k njihovi uporabi.	SeKV-ZIT je mnenja, da bi vlada morala z uredbo - kot pri ZInfV z Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev - določiti SUVI in SUNP dokumentacijo, poleg objav na spletni strani pa pošiljati tudi obvestila na spletne naslove zavezancev, vključno z opozorili na relevantne dokumente ENISA Imamo že dobro prakso, ki bi jo lahko ohranili in sicer 12. člen obstoječega zakona ZInfV.	
25. člen (obveznost priglašanja in obveščanja)		
(1) Bistveni in pomembni subjekti pristojni skupini CSIRT brez nepotrebnega odlašanja v skladu s prvim in drugim odstavkom 26. člena tega zakona priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Pri tem se incident šteje za pomembnega, če: - je zadevnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube; - je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode. (2) Bistveni in pomembni subjekti pri priglašanju iz prejšnjega odstavka upoštevajo morebitne izvedbene akte Evropske komisije iz prvega pododstavka enajstega odstavka 23. člena Direktive 2022/2555, s	SeKV-ZIT močno zagovarja, da potrebujemo tudi izvedbeni predpis – uredba je potrebna, glede prijavljanja incidentov, ukrepanja, odzivni časi, itd. V izvedbenem predpisu je potrebno opredeliti prvo zaznavo, prvo poročilo, dodatne zaznave, končno poročilo in ugotovitve skupaj z roki.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
katerimi ta podrobneje določi vrsto informacij, obliko in postopek priglasitve ter prostovoljne priglasitve in obvestila.		
26. člen (postopek priglasitve pomembnih incidentov)		
(1) Bistveni in pomembni subjekti za namen priglasitve pomembnih incidentov iz prvega in drugega odstavka prejšnjega člena pristojni skupini CSIRT predložijo: 1. brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po zaznavi incidenta, zgodnje opozorilo, iz katerega je po potrebi razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali bi lahko imel čezmejni vpliv; 2. brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po zaznavi pomembnega incidenta, priglasitev incidenta, s katero se po potrebi posodobijo informacije iz točke ena in navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter, kadar so na voljo, kazalniki ogroženosti; 3. na zahtevo skupine CSIRT vmesno poročilo o ustreznih posodobitvah stanja; 4. končno poročilo, najpozneje v enem mesecu po predložitvi priglasitve incidenta iz točke dva, ki vključuje naslednje: – podroben opis incidenta, vključno z njegovo resnostjo in vplivom;	(1) Postopek priglasitve t.i. "pomembnih incidentov" je določen zelo natančno in strokovno korektno. Kakšen pa bo postopek priglasitve (časovni roki, vsebina priglasitve, ocena vplivov..-) incidentov, ki ne bodo izpolnjevali meril za razvrstitev med "pomembne". Menimo, da je prijave tistih, ki niso zavezanci oz. ponudniki bistvenih storitev potrebno še definirati v zakonu. Po določbah člena 23(3) NIS2 direktive oz. 25/1 člena predmetnega predloga zakona, je incident pomemben, če: a. *je zadevnemu subjektu povzročil ali bi mu lahko povzročil **znatne operativne motnje** pri opravljanju storitev ali **finančne izgube**;* *(b) je vplival ali bi lahko vplival na druge fizične ali pravne osebe s **povzročitvijo precejšnje premoženjske ali nepremoženjske škode**.* Potrebna je določitev postopka za priglasitev vseh incidentov in tudi način poročanja o	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
– vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident; – izvedene blažilne ukrepe in take ukrepe v teku; – po potrebi čezmejni vpliv incidenta; 5. v primeru incidenta, ki je ob predložitvi končnega poročila iz točke štiri še vedno v teku, priglasitveni subjekt predloži poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta. (2) Ne glede na določbo 2. točke prejšnjega odstavka mora ponudnik storitev zaupanja v zvezi s pomembnimi incidenti, ki vplivajo na zagotavljanje njegovih storitev, o tem brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po zaznavi pomembnega incidenta, uradno obvesti pristojno skupino CSIRT.	incidentu, o katerem je potrebno obvestiti več pristojnih državnih organov, npr. poleg URSIV še Informacijskega pooblaščenca, AKOS, Urad Vlade RS za varovanje tajnih podatkov, Inšpektorat za informacijsko družbo ipd. (2) Izvedbeni akti, ki bodo izdani na podlagi DORA (osnutki so že v javni obravnavi), v določenih primerih predvidevajo bistveno krajše roke obveščanja/odzivanja na incidente. Npr. 4 ure. Potrebna je uskladitev.	
30. člen (dogovori o izmenjavi informacij o KV)		
(2) Izmenjava informacij poteka v skupnostih zavezancev ter, kadar je to ustrezno, z njihovimi dobavitelji ali ponudniki storitev. Taka izmenjava se izvaja na podlagi dogovorov o izmenjavi informacij o kibernetski varnosti, ob upoštevanju morebitne občutljive narave informacij, ki se izmenjujejo. Pri sklenitvi dogovorov o izmenjavi informacij se kar najbolj upoštevajo dobre prakse in smernice ENISA.	(2) SeKV-ZIT zagovarja, da je predmetno izmenjavo informacij med zavezancem in njegovim zunanjim izvajalcem (obdelovalcem, tretjim dobaviteljem IKT storitev…) potrebno vključiti kot obvezno klavzulo v pogodbo med zavezancem in zunanjim izvajalcem. (4) Zanima nas kaj je namen oz. dodana vrednost obveščanja pristojnega	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
(4) Bistveni in pomembni subjekti morajo obvestiti pristojni nacionalni organ in za njih pristojno skupino CSIRT o svojem sodelovanju pri dogovorih o izmenjavi informacij o kibernetski varnosti iz drugega odstavka tega člena, po sklenitvi takih dogovorov ali, kadar je potrebno, o odstopu od dogovora, ko odstop začne veljati. Skrbnik takšnega dogovora posreduje obvestilo pristojnim organom v roku 15 dni od nastanka dogodka.	nacionalnega organa, kadar je izmenjava informacij del pogodbenega razmerja med naročnikom in izvajalcem IKT storitev?	
31. člen (prostovoljna priglasitev)		
(1) Zavezani subjekti lahko poleg obvezne priglasitve iz 26. člena tega zakona skupinam CSIRT prostovoljno priglasijo incidente, kibernetske grožnje in skorajšnje incidente in jim predložijo ustrezne informacije. Pri prostovoljni priglasitvi se glede skupine CSIRT, ki se ji priglaša, smiselno uporabljata drugi in tretji odstavek 12. člena tega zakona. (2) Subjekti, ki niso zavezanci po tem zakonu, ne glede na to, ali spadajo na področje uporabe tega zakona, lahko prostovoljno priglasijo pomembne incidente, kibernetske grožnje in skorajšnje incidente skupini CSIRT SI-CERT in ji predložijo ustrezne informacije.	(1) Razumemo, da incidente, ki niso "pomembni", tudi zavezanci priglasijo prostovoljno. Posebej bi morali izpostaviti, da ta določba ne vpliva na določbe drugih predpisov, ki urejajo postopke prijave kršitev obdelave/obravnavanja podatkov (npr. osebnih, tajnih) oz. ogrožanja sistemov za obdelavo/obravnavo omenjenih podatkov (2) Med subjekti, ki niso zavezanci, bi kazalo v povezavi s priglasitvijo incidentov posebej obravnavati zunanje izvajalce storitev IKT za ponudnike bistvenih oz. pomembnih storitev. Npr. na način, kot za prijavo kršitve varnosti osebnih podatkov določa 33. člen GDPR, ki za poročanje o incidentu pooblašča (le) upravljavca, obdelovalcu pa nalaga, da po seznanitvi z incidentom o tem brez nepotrebnega odlašanja obvesti upravljavca.	Dodatna razlaga: Razmerja med zavezancem in njegovim zunanjim izvajalcem pa v ZInfV-1 ne bi kazalo urediti le v povezavi z obravnavanjem incidentov, ampak širše. Za zgled bi lahko bila Uredba DORA, ki je (že) specialni sektorski predpis za izvedbo NIS2 direktive, podobno kot bo ZInfV-1 nacionalni predpis za izvedbo NIS2 direktive. V zvezi z zunanjimi izvajalci oz. "tretjimi osebami na področju IKT", kot jih imenuje DORA, bi kazalo iz omenjene EU uredbe smiselno prevzeti zlasti določbe členov 28 - 30, ki določajo splošna načela, izdelavo ocene tveganj glede sklenitve pogodbe v zvezi s storitvami IKT, ki podpirajo kritične ali pomembne funkcije ter opredeljujejo ključne določbe, ki jih naj bi vsebovala pogodba med zavezancem in njegovim zunanjim izvajalcem storitev IKT.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
32. člen (vrednotenje incidenta in ukrepanje)		
(1) Priglašene incidente ob njihovem reševanju vrednoti pristojna skupina CSIRT. V primeru, da ima organ državne uprave zagotovljene zmogljivosti vsaj na ravni varnostno operativnega centra, pristojna skupina CSIRT opravi vrednotenje po posvetu z varnostno operativnim centrom. V kolikor pristojni nacionalni organ ugotovi, da ocena ne odraža realnega stanja ali so bila ugotovljena nova dejstva, lahko incident prevrednoti. Varnostne dogodke in incidente se vrednoti v naslednje stopnje s poimenovanjem: - C6 - C5 - C4 - C3 - C2 - C1	SeKV-ZIT predlaga črtanje (a) četrtega do osmega odstavka 32. člena in (b) sedmega do desetega odstavka 33. člena saj niso v skladu z NIS 2 in določajo preširoka pooblastila ter so tudi v nasprotju z načelom jasnosti in določnosti predpisov (kot elementa načela pravne države iz 2. člena Ustave). Sprašujemo se ali so te pristojnosti URSIV-a dejansko potrebne?	Takšne pristojnosti so preširoke, nedefinirane in se z njimi predlog odmika od NIS 2 in predlagamo, da se takšne izrecne pristojnosti črtajo. Tako široko blanketno pooblastilo (da se lahko odredijo kakršnikoli ukrepi) je verjetno v nasprotju z ustavo in problematično v praksi. Skladno z drugim odstavkom 120. člena Ustave upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov (legalitetno načelo), kar vključuje tudi zahtevo po vsebinski vezanosti uprave na ustavo in zakon, ki zagotavlja, da se posamezniki in pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali. Skladno s 87. členom Ustave pa lahko pravice in obveznosti državljanov ter drugih oseb državni zbor določa le z zakonom, kar predstavlja tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon. Predlagatelj je nalaganje obveznosti v celoti prepustil URSIV, kar je v nasprotju z ustavnim načelom legalitete,

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
		omejitve pa lahko posegajo tudi na trg (torej tudi na prosto nastopanje dobaviteljev na trgu) in gre s tem tudi za omejitev oziroma določitev načina uresničevanja svobodne gospodarske pobude (74. člen Ustave RS). Problematična je tudi odprtost in splošnost 32. in 33. člena.
36. člen (sodelovanje na področju kibernetske obrambe)		
(3) Pristojni nacionalni organ opravi izbor kandidatov za prostovoljce iz prejšnjega odstavka in zanje sproži postopek varnostnega preverjanja po zakonu, ki ureja tajne podatke. Po opravljenem varnostnem preverjanju jih uvrstitvi na seznam prostovoljcev, ki ga vodi. Ta seznam vsebuje: - ime, priimek in rojstne podatke; - davčno številko; - naziv, naslov, telefonsko številko ter elektronski naslov; - doseženo izobrazbo; - morebitno zaposlitev; - znanja in kompetence.	Namen in rezultat varnostnega preverjanja po ZTP je preverba, ali pri preverjani osebi obstajajo varnostni zadržki za dostop do tajnih podatkov in, če jih ni, izdaja dovoljenja za dostop do tajnih podatkov določene stopnje tajnosti. Ali se bo tudi predlagani postopek VP končal z (ne)izdajo dovoljenja za dostop do TP? Po našem mnenju je potrebno bolj konkretizirati predlog in upoštevati pravila o osebnih podatkih.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
40. člen (splošne določbe)		
(1) Za nadzor nad izvajanjem določb tega zakona, na njegovi podlagi sprejetih predpisov in nad izvršitvijo upravnih odločb, izdanih na podlagi četrtega ali petega odstavka 32. člena sedmega odstavka 33. člena tega zakona, nad izvršitvijo odredb, izdanih na podlagi sedmega odstavka 32. člena in devetega odstavka 33. člena tega zakona, so pristojni inšpektorji za informacijsko varnost pristojnega nacionalnega organa (v nadaljnjem besedilu: inšpektor).	SeKV-ZIT je menja, da je 40. člen presplošen in gre preko obsega NIS 2. Predlagamo, da se inšpekcijske / nadzorstvene pristojnosti omejijo na pristojnosti, ki jih predvideva NIS 2 (ki so že rezultat tehtanja med drugim tudi z vidika sorazmernosti in procesnih jamstev) in so tako in tako relativno široke. V nasprotnem (ko gre za dodatno širjenje pristojnosti) verjetno ne bo podana sorazmernost in je ureditev problematična z vidika ustavnih jamstev in konvencijskih pravic. Navedeno velja tudi za preostale določbe glede nadzora in inšpekcijskih pristojnosti.	Kot je razumeti, naj bi bili inšpektorji za informacijsko varnost v sestavi pristojnega nacionalnega organa. Ta organ – URSIV – ima po ZInfV-1 vrsto drugih vlog/dolžnosti, ki lahko vplivajo oz. so lahko konfliktu z neodvisnim inšpekcijskim nadzorom.
41. člen (nadzor bistvenih subjektov)		
(1) Ukrepi, ki jih inšpektor naloži bistvenim subjektom v zvezi z obveznostmi iz tega zakona morajo biti učinkoviti, sorazmerni in odvračilni, pri čemer se upoštevajo okoliščine posameznega primera. (2) Inšpektor je pri izvajanju svojih nadzornih nalog pri bistvenih subjektih pooblaščen za to, da: 6. zahteva ~~dostop do prostorov~~, podatkov, dokumentov in informacij, potrebnih za opravljanje njegovih nadzornih nalog;	Predlagamo, da se v drugem odstavku, v 6. točki briše »dostop do prostorov«, saj navedeno ni v skladu z NIS 2. Relevantna določba NIS 2 govori zgolj o dostopu do podatkov, dokumentov in informacij: »zahtevajo dostop do podatkov, dokumentov in informacij, potrebnih za opravljanje njihovih nadzornih nalog;« tako imenovana »hišna preiskava« oz. dostop do prostorov (preko obsega dostopa do podatkov, dokumentov in informacij), pa bi bil problematičen z vidika Ustave RS. Enako velja tudi za 43. člen glede pomembnih subjektov.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
42. člen (ukrepi nadzora bistvenih subjektov)		
(1) Inšpektorji so pri izvajanju nadzora v zvezi z bistvenimi subjekti pooblaščeni, da: 1. izdajo opozorila o kršitvah tega zakona; 2. izdajo zavezujoča navodila, tudi v zvezi z ukrepi za preprečitev ali odpravo incidenta, roki za njihovo izvedbo in poročanjem o tem, ali odredbo, s katero od bistvenih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve tega zakona; 3. bistvenim subjektom odredijo, naj prenehajo z ravnanjem, ki krši ta zakon, in naj tega ravnanja ne ponovijo več; 4. bistvenim subjektom odredijo, naj na določen način in v določenem roku poskrbijo, da bodo njihovi ukrepi za obvladovanje tveganj za kibernetsko varnost v skladu s 20. členom tega zakona, oziroma naj izpolnijo obveznosti poročanja iz 25. in 26. člena tega zakona; 5. bistvenim subjektom odredijo, naj obvestijo fizične ali pravne osebe, v zvezi s katerimi opravljajo storitve ali izvajajo dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo; 6. bistvenim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi revizije varnosti;	Ukrepe nadzora bistvenih subjektov je potrebno po mnenju SeKV-ZIT jasneje definirati in opredeliti.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
7. imenujejo pooblaščeno osebo z natančno opredeljenimi nalogami v določenem obdobju, ki spremlja izpolnjevanje 20., 25. in 26. člena tega zakona s strani bistvenih subjektov; 8. bistvenim subjektom odredijo, naj na določen način objavijo kršitve tega zakona; 9. naložijo globo na podlagi 53. člena tega zakona poleg katerega koli od ukrepov iz točk 1. do 8. tega odstavka.		
43. člen (nadzor pomembnih subjektov)		
(1) Inšpekcijski nadzor pomembnega subjekta se izvede, če inšpektor prejme dokaze, indice ali informacije, da pomembni subjekt ne izvaja ukrepov za obvladovanje tveganj kibernetske varnosti v skladu s predpisanimi obveznostmi iz tega zakona oziroma, da ne izpolnjuje obveznosti v zvezi s obveščanjem o kibernetskih incidentih na predpisan način in v predpisanih rokih ali da ne ravna po zahtevah pristojnega nacionalnega organa iz tega zakona. (6) Inšpektor sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554. Pri tem inšpektor zagotovi, da o nadzoru pomembnega subjekta, ki je imenovan za ključnega tretjega ponudnika storitev IKT na podlagi člena 31 Uredbe (EU) 2022/2554, o tem obvesti nadzorniški forum, ustanovljen na podlagi člena 32(1) Uredbe (EU) 2022/2554.	Zanima nas kakšna je razlika pri nadzoru bistvenih in pomembnih subjektov v 41, in 43. členu? (6) Predlagamo uporabo DORA.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
45. člen (ocena skladnosti)		
(1) Odgovorne osebe zagotovijo, da bistveni subjekti izvajajo oceno skladnosti sprejetih ukrepov za obvladovanje tveganj kibernetske varnosti iz tega zakona in da pomembni subjekti izvajajo oceno skladnosti takšnih ukrepov. (2) Izvajanje ocene skladnosti morajo bistveni subjekti opraviti najmanj enkrat na dve leti, pred potekom roka pa, če to zahteva inšpektor ali v primeru pojava pomembnega incidenta. Ocena skladnosti se izvaja kot revizija informacijske varnosti ali v okviru revizije poslovanja, ki se izvaja na podlagi drugih predpisov in vključuje tudi področje informacijske varnosti iz tega zakona in na podlagi tega zakona izdanih podzakonskih predpisov ali izvedbenih aktov Evropske komisije. (3) Pomembni subjekti morajo izvesti oceno skladnosti na zahtevo inšpektorja ali v primeru pojava pomembnega incidenta. (4) Preizkušeni revizor za bistvenega ali pomembnega subjekta pripravi poročilo o izvedeni oceni skladnosti.	Vezano na vlogo preizkušenega revizorja po 45/4. členu. Menimo, da ni potrebe, da poročilo pripravi preizkušen revizor, posebej ne ob upoštevanju definicije iz 5/39. člena predloga (glej tudi pripombe k definiciji preizkušenega revizorja. Menimo, da je po določbah NIS2 ključno, da pregled opravi neodvisen subjekt (lahko tudi neodvisna oseba, ki ji je zagotovljena neodvisnost znotraj zavezanca). Mešajo se tudi funkcije regulatorja in inšpekcije. SeKV-ZIT je mnenja, da je potrebno natančneje opredeliti zahteve. Preizkušeni revizor nima enako poglobljenega znanja o skladnosti z zahtevami kibernetske varnosti, kot na primer vodilni presojevalec po standardu ISO/IEC 27001	Dodatna pojasnila: Če "oceno skladnosti" prevedemo v ISO terminologijo, govorimo o notranji presoji in vodstvenem pregledu, v primeru pridobitve certifikata skladnosti z ISO standardom, ki tovrstno potrditev skladnosti določa in omogoča - npr. ISO/IEC 27001:2022,ki je najbolj prepoznaven standard na področju varovanja informacij -, pa govorimo o zunanji presoji akreditiranega certifikacijskega organa, ki v presojani organizaciji preveri, ali dejansko in na ustrezen način izvaja kontrole, ki jih za želeno skladnost zahteva določen standard. Pogoj za izvedbo ocene skladnosti je torej nabor/seznam zahtev/kontrol, ki predstavljajo podlago za oceno skladnosti. Ustvarjanje takega seznama iz določb ZInfV-1 ne more biti prepuščeno posameznemu zavezancu, ampak mora biti nedvoumno opredeljen v ustreznem (izvedbenem) predpisu. Velja strokovna ocena, da posest certifikata ISO/IEC 27001:2022 "pokriva" cca. 70% zahtev NIS2 direktive. Obstajajo tudi korelacijske tabele med zahtevami NIS2 in ISO/IEC 27001:2022 ter 27002:2022, ki so v pomoč pri identificiranju cca. 30% preostalih (residualnih) tveganj. Posest omenjenega certifikata in tudi nekaterih drugih potrdil o skladnosti, ki jih izdajajo akreditirani certifikacijski organi, bi morala imeti nek učinek na oceno skladnosti.Predvidena ocena skladnosti je, če se ponovno opremo na ISO/IEC

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
		27001, izjava o uporabnosti/skladnosti (*Statement of Applicability;* SoA), v kateri organizacija navede, s katerimi ukrepi in politikami je izvedla zahtevane kontrole iz priloge A omenjenega standarda.
46. člen (samoocena skladnosti)		
(1) Izvajanje samoocene skladnosti morajo pomembni subjekti opraviti najmanj enkrat na dve leti. (2) Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomemben subjekt izpolnjuje zahteve, predpisane s tem zakonom, pomembni subjekti sestavijo izjavo o skladnosti, ki vsebuje potrebne elemente samoocenjevanja skladnosti. (3) Pomembni subjekti morajo izjavo iz prejšnjega odstavka tega člena brez odlašanja predložiti inšpektorju, v osmih dneh od njene sestave. (4) Stroške izvajanja samoocene skladnosti nosijo pomembni subjekti.	45. in 46. člen glede obveznosti pomembnih subjektov nista konsistentna. Ali je to razumeti kot neko stalno obliko poročanja? Kaj pa bo inšpektorat počel s prejetimi samoocenami? Ali ne bi bilo ustrezneje, da pomembni subjekt zadnjo ali zadnji dve samooceni na poziv predloži inšpektorju v okviru inšpekcijskega postopka. Skladno z ZIN lahko inšpektor skladnost samoocene z dejanskim stanjem preveri le v okviru konkretnega inšpekcijskega postopka. Kateremu inšpektorju? Mora odpreti inšpekcijski postopek. Kaj pa v primeru, če samoocena ne potrjuje ustreznosti?	
48. člen (kršitve, ki pomenijo kršitve varstva osebnih podatkov)		
(1) Inšpektor o obravnavi zadev iz prvega odstavka 40. člena tega zakona, katerih posledica je kršitev varstva osebnih podatkov, obvešča Informacijskega pooblaščenca brez nepotrebnega odlašanja. Za namen pravočasnega ukrepanja v smeri zagotavljanja odprave kršitev varstva osebnih podatkov inšpektor Informacijskega pooblaščenca obvešča tudi v primerih suma kršitve varstva osebnih podatkov.	Zanima nas ali je podobnih situacij še kaj na primer po Uredbi eIDAS?	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
53. člen **(prekrški bistvenih subjektov)**		
(4) Z globo od 1.000,00 eurov do 10.000,00 eurov, se kaznuje pravna oseba, če: - ne izpolni obveznosti iz drugega ali tretjega odstavka 7. člena tega zakona, - ne izpolni obveznosti iz drugega ali tretjega odstavka 19. člena tega zakona, - ne izpolni obveznosti iz prvega odstavka 22. člena tega zakona, - ne izpolni obveznosti iz tretjega odstavka 23. člena tega zakona, - ne izpolni obveznosti iz prvega odstavka 24. člena tega zakona, - ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 28. člena tega zakona - ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 29. člena tega zakona, - ne izpolni obveznosti iz prvega, drugega, tretjega, petega ali šestega odstavka 45. člena tega zakona, - ne izpolni obveznosti iz tretjega odstavka 47. člena tega zakona.	SeKV-ZIT opozarja na nekonsistentnost z angleškim prevodom, saj NIS 2 določa zgornji prag glob! Napako je potrebno odpraviti. Predvidene globe so nesorazmerne in gredo preko obsega, ki ga predvideva NIS 2. NIS 2 direktiva ne določa minimalnih glob, predvideva pa za najhujše kršitve globo do maksimalno 2% prometa (oziroma 10 mio EUR). Glede na to, da NIS 2 direktiva ne predpisuje minimalnih glob (zgolj maksimalno globo), in da lahko gre glede na relativno abstraktnost dikcije ZInfV-1 in širok krog potencialnih kršitev, na spektru od morebitnih prekrškov povsem neznatnega pomena do hudih prekrškov, bi bilo smiselno, da se bodisi ne predpisuje minimalna globa, ali da je ta (na spodnjem delu razpona) predpisana v nominalnem znesku. Predlagamo, da se možnost izreka globe do 2% prometa rezervira za primere, ki jih predvideva NIS 2 direktiva in takšna izjemno huda sankcija ne širi preko dometa NIS 2. Glede na to, da NIS 2 predvideva zgolj globo za kršitev iz 21. člena NIS 2 (ukrepi za obvladovanje	Vsekakor se zdi primerneje, da se najnižja globa ne bi določala, ali da bi bila najnižja globa določena zgolj v nominalnem znesku (ne v odstotku od prometa, saj so globe določene v odstotku od prometa primerjalno rezervirane za najtežje kršitve). Primerjalno-pravno je bilo prvo področje, kjer so se uveljavile kazni v odstotku od prometa na področju konkurenčnega prava in le-to določa zgolj najvišjo sankcijo (npr. glejte 85. člen ZPOmK-2 do deset odstotkov letnega prometa), ne pa minimalnega zneska, kar omogoča širše polje diskrecije ob izreku sankcije. Drugačna ureditev ne bi zadostila kriteriju sorazmernosti in bi bila potencialno protiustavna. ZInfV-1 dodatno predvideva globo v odstotku od prometa tudi za kršitve 21. člena (dnevniški zapisi), 23. člena (certifikacijske sheme), 25. člena (tako da globa ni zamejena na 6. in 7. odstavek) ter 26. člen, torej bistveno manj hude kršitve, kar pa ne more biti v skladu s kriterijem

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
	tveganj za kibernetsko varnost), ki bi ga implementiral 20. člen ZINfV-1, in 23. člen NIS 2 (Obveznosti poročanja o incidentih), ki se nanaša na obveznost sporočanju prejemnikom storitev, ki bi jo implementiral 6. in 7. odstavek 25. člena ZInfV-1., predlagamo, da se tudi ZInfV-1 omeji na navedeni dve situaciji.	sorazmernosti in je posledično potencialno neustavno.
54. člen **(prekrški pomembnih subjektov)**		
(4) Z globo od 1.000,00 eurov do 10.000,00 eurov, se kaznuje pravna oseba, če: - ne izpolni obveznosti iz drugega ali tretjega odstavka 7. člena tega zakona, - ne izpolni obveznosti iz drugega ali tretjega odstavka 19. člena tega zakona, - ne izpolni obveznosti iz prvega odstavka 22. člena tega zakona, - ne izpolni obveznosti iz tretjega odstavka 23. člena tega zakona, - ne izpolni obveznosti iz prvega odstavka 24. člena tega zakona, - ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 28. člena tega zakona - ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 29. člena tega zakona,	Naš komentar je enak kot pri 53. členu.	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
- ne izpolni obveznosti iz prvega, drugega, tretjega, petega ali šestega odstavka 45. člena tega zakona, - ne izpolni obveznosti iz tretjega odstavka 47. člena tega zakona.		
56. člen **(vzpostavitev samoregistracije, seznamov in obveščanje)**		
(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz 6. člena tega zakona po prvem odstavku 7. člena tega zakona v roku dveh mesecev od uveljavitve tega zakona. (2) Zavezanci iz 6. člena tega zakona opravijo prvo registracijo po mehanizmu za samoregistracijo v roku dveh mesecev od njegove vzpostavitve v skladu s prejšnjim odstavkom.	SeKV-ZIT meni, da so roki za izvedbo prekratki in močno zagovarja daljše časovno obdobje za skladnost. Prehodno obdobje je treba zapisati v ZInfV-1. Zanima nas, kdaj bodo morala biti podjetja skladna z ZInfV-1 po mnenju URSIV-a?	
57. člen **(sprejem ukrepov za obvladovanje tveganj)**		
Bistveni in pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost iz 20. člena tega zakona v roku šestih mesecev od uveljavitve tega zakona.	Predvideni rok za sprejetje vseh ukrepov za obvladovanje tveganj za kibernetsko varnost pri zavezancih je odločno prekratek. Zavezanci bodo omenjene ukrepe zelo težko sprejeli, če vlada ne bo izdala nekaterih predpisov, ki so predvideni oz. bi morali biti predvideni v predmetnem zakonu. Predviden rok "striže" z rokom iz prvega odstavka 59. člena predmetnega zakona. Da bi nek subjekt začel s pripravo in sprejemanjem ukrepov iz 20. člena tega zakona, se mora najprej "prepoznati" kot zavezanec po	Glede na rok za prvo obveščanje Komisije EU o številu bistvenih in pomembnih subjektov, ki se izteče 17. aprila 2025, je razumljivo, da se URSIV-u mudi. Ampak NIS 2 direktiva velja že od 16.1.2023, nacionalne predpise , potrebne za uskladitev z direktivo morajo države članice sprejeti do 17.10.2024, uporabljati pa od 18.10.2024 dalje.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
	ZInfV-1. Če pogledamo roke iz prvega in drugega odstavka 56. člena, lahko ugotovimo, da bodo imeli zavezanci glede na rok za vzpostavitev mehanizma za evidentiranje in izvedbo "samoregistracije" še dva meseca časa za sprejetje ukrepov. Pri čemer ni jasno določeno, kdaj bo vlada, če sploh, na podlagi ZInfV-1 sprejela predpis, ki bi bil ekvivalent Uredbi o varnostni dokumentaciji in varnostnih ukrepih…, sprejeti na podlagi ZInfV.	
59. člen (izdaja podzakonskih predpisov in strategije)		
(1) Vlada izda predpise, ki so po tem zakonu obvezni, v enem letu od uveljavitve tega zakona.	SeKV-ZIT je mnenja, da bi bilo nujno zaradi večje preglednosti in jasnosti, da so členi, katerih določbe bodo predmet obveznega podzakonskega urejanja, jasno našteti. Zakaj je to nujno, je razvidno iz 57. člena oz. pripombe na omenjeni člen.	V posameznem členu naj bo navedeno, kdaj bo URSIV/Vlada sprejel posamezen izvedbeni predpis.
61. člen (spremembe in dopolnitve ZEKom)		
(2) V Zakonu o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O): □ v prvem odstavku 116. člena se za besedama »ta omrežja« dodata besedi »in storitve«; □v prvem stavku drugega odstavka 116. člena se besedi »prejšnjega člena« nadomestita z besedilom: »zakona, ki ureja informacijsko varnost«; - v prvem stavku četrtega odstavka 116. člena se besedilo »tretjega odstavka prejšnjega člena"	SeKV-ZIT predlaga, da se ne širi dometa 116. člena ZEKom-2. Predlog bi bistveno širil ta restriktivni ukrep, posegal v svobodo gospodarske pobude (v nasprotju z načelom sorazmernosti), za takšno spremembo pa ni niti podlage v NIS 2.	Predlog spremembe 116. člena ZEKom-2 bistveno širi domet te določbe in sicer iz operaterjev mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja upravljavcem kritične infrastrukture, na praktično vse operaterje, ki zagotavljajo kakršnekoli storitve upravljavcem kritične infrastrukture, kar je bistveno širši krog (verjetno vsi operaterji zagotavljajo

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
nadomesti z besedilom »vseh varnostnih tveganj v skladu z zakonom, ki ureja informacijsko varnost« v petem odstavku 116. člena se za besedama »predmetnih omrežij« dodata besedi »in storitev«; □ v četrtem odstavku 124. člena se besedilo za vejico, ki se glasi: »se uporablja določba petega odstavka 115. člena tega zakona« nadomesti z besedilom »mora biti ta vsaj enkrat letno pregledan. Za njegovo sprejetje in morebitne spremembe ali posodobitve je potrebna predhodna odobritev pristojnih organov, odgovornih za delovanje centrov za sprejem komunikacije v sili.«; □ v 128. členu se prva vejica nadomesti s piko in briše besedilo »razen določb 120. in 121. člena tega zakona, kjer nadzor izvaja organ, pristojen za informacijsko varnost.«; □v prvem odstavku 287. člena se brišeta besedilo »ali organa, pristojnega za informacijsko varnost na podlagi 128. člena tega zakona« prvega stavka in tretji stavek; □v 288. členu se za besedo »Agencija« vejica nadomesti z veznikom »in«, besedilo »ter organ, pristojen za informacijsko varnost, se morajo« pa se nadomesti z besedama »se morata«; □v 289. členu se črta tretji odstavek; □v 299. členu se črtajo 22., 23., 24., 26., 27., 28., 29. in 30. točka.		kakšno storitev kateremu od upravljavcev kritične infrastrukture). Širitev potencialne prepovedi iz petega odstavka 116. člena ZEKom-2 na vse takšne operaterje je nesorazmerna in protiustavna. Istočasno »storitve« sploh niso opredeljene, torej na kakšne storitve naj bi se predlog nanašal in ni kakršnekoli omejitve, da bi šlo za »kritične« storitve. Takšen predlog bi tudi zahteval vnovično priglasitev po mehanizmu TRIS, saj bi šlo za spremembo (bolj restriktiven poseg) v primerjavi z že priglašenim besedilom ZEKom-2 v okviru TRIS mehanizma.

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
PRILOGA I VISOKO KRITIČNI SEKTORJI		
8. Digitalna infrastruktura - ponudniki storitev zaupanja	Potrebna je bolj jasna definicija ponudnikov storitev "zaupanja".	
PRILOGA II DRUGI KRITIČNI SEKTORJI		
Drugi komentarji:	NIS 2 ne določa obveznosti za raziskovalne ustanove, vendar peti odstavek 2. člena NIS 2 dopušča, da lahko države članice določijo, da so zavezanci tudi ustanove, ki izvajajo kritične raziskovalne dejavnosti. Glede na to, da pravo EU ne zahteva, da bi se moral ZInfV-1 uporabljati tudi za te ustanove, bi bilo v zvezi z navedeno razširitvijo uporabe NIS 2 potrebno izvesti tudi presojo posledic za gospodarstvo in upoštevati načelo sorazmernosti. Ne zdi se skladno z načelom enakosti in načelom sorazmernosti, da bi se ZInfV-1 uporabljal za vse raziskovalne ustanove, temveč bi bilo navedeno (če bo predlagatelj utemeljil in dokazal, zakaj bi bila takšna ureditev primerna, nujna in sorazmerna v ožjem pomenu) omejiti na raziskovalne ustanove, ki izvajajo »kritične raziskovalne dejavnosti«. Npr. če je mogoče videti utemeljeni	

Predlog URSIV	Pripombe SeKV-ZIT	Utemeljitev
	interes zakaj se pri raziskovalni ustanovi, ki se ukvarja z jedrskimi raziskavami ali na primer upravlja jedrski reaktor, zahteva višja stopnja kibernetske varnosti, takšne situacije ni mogoče enačiti z raziskovalnimi ustanovami, ki niso varnostno občutljive oziroma »kritične« (npr. sociološke raziskave). Predlagamo ustrezno zamejitev skladno z NIS 2 direktivo.	