EVA 2023-1544-0005

OSNUTEK PREDLOGA
15. 5. 2024

II. BESEDILO ČLENOV

ZAKON
O INFORMACIJSKI VARNOSTI

I. Splošne določbe

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 in prostovoljno priglasitev incidentov. Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu vključno za področje certificiranja kibernetske varnosti.

2. člen
(namen zakona)

(1) Namen zakona je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti vključno s krepitvijo zaupanja v proizvode IKT, storitve IKT in postopke IKT ter njihove varnosti v Republiki Sloveniji na področjih, ki so bistvenega 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 (EU) 2022/2555).

(3) S tem zakonom se ureja izvajanje 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) (UL L št. 151 z dne 7. 6. 2019, str. 15; v nadaljnjem besedilu: Uredba (EU) 2019/881).

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 ali letno bilančno vsoto vsaj 10 milijonov evrov.

(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;
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.

(4) Ta zakon se uporablja tudi za subjekte, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost.

(5) Ta zakon se uporablja tudi za organe, ki v skladu z državnimi načrti zaščite in reševanja izvajajo naloge na področju zaščite in reševanja, v kolikor ti organi že niso zajeti na podlagi prejšnjih odstavkov tega člena.

(6) Ta zakon se uporablja tudi za subjekte lokalne samouprave in sicer za mestne občine in občine, ki imajo sedeže v krajih, kjer so sedeži upravnih enot.

(7) Ta zakon se ne uporablja za subjekte, ki jih je Republika Slovenija izvzela s področja uporabe Uredbe (EU) 2022/2554 v skladu s četrtim odstavkom 2. člena prej navedene uredbe.

(8) Ta zakon ne posega v izvajanje predpisov s področja varstva osebnih podatkov in zasebnosti na področju elektronskih komunikacij, s področja boja proti spolni zlorabi otrok in proti izdelavi, razširjanju in hrambi gradiva, ki prikazuje spolno zlorabo otrok ter predpisa o napadih na informacijske sisteme ter s področja kritične infrastrukture.

(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.

(10) Zahteve iz prejšnjega odstavka se štejejo za enakovredne obveznostim iz tega zakona, kadar:

- imajo ukrepi za obvladovanje tveganj za kibernetsko varnost vsaj enakovreden učinek kot ukrepi iz prvega in drugega odstavka 21. člena tega zakona ali
- področni predpis določa takojšen, po potrebi samodejen in neposreden dostop do priglasitev incidentov za skupine CSIRT, pristojni nacionalni organ oziroma enotno kontaktno točko iz tega zakona in kadar so zahteve za priglasitev pomembnih incidentov po učinku vsaj enakovredne tistim iz prvega do šestega odstavka 25. člena tega zakona.

(11) Pri izvajanju devetega in prejšnjega odstavka tega člena se upoštevajo smernice, Evropske komisije o uporabi člena 4 (1) in (2) Direktive (EU) 2022/2555. Pristojni nacionalni organ vodi ažuren seznam neposredno uporabljivih EU predpisov in nacionalnih predpisov, ki so po učinku enakovredni določbam tega zakona. Predlog za uvrstitev na seznam, ki mora biti v skladu z devetim in prejšnjim odstavkom tega člena ter ob upoštevanju smernic iz tega odstavka, posreduje pristojnemu nacionalnemu organi za posamični predpis pristojno resorno ministrstvo ali regulatorni organ, če je pooblaščen za sprejem ustreznega akta. Pristojni nacionalni organ po presoji izpolnjevanja pogojev uvrsti posamični EU ali nacionalni predpis na seznam, ki se objavi na spletni strani pristojnega nacionalnega organa.

(12) Ta zakon se v delu, ki se nanaša na področje certificiranja kibernetske varnosti, uporablja tudi za druge fizične in pravne osebe, ki niso bistveni ali pomembni subjekti po tem zakonu, ki jih zadeva Uredba (EU) 2019/881 v delu, ki ureja certifikacijski okvir za kibernetsko varnost.

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. Izmenjava 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.

(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. Predstojnik pristojnega nacionalnega organa podrobneje predpiše organizacijske in logično tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenja zbirk podatkov katerih upravljavec je pristojni nacionalni organ. Uslužbenec pristojnega nacionalnega organa mora varovati varovane podatke pristojnega nacionalnega organa tudi po prenehanju delovnega razmerja.

(4) Pri posredovanju ali izmenjavi podatkov in informacij na podlagi tega zakona se upošteva tudi sporazume o nerazkritju informacij in neformalne sporazume o nerazkritju informacij, kot je semaforski protokol.

(5) Obveznost izmenjave podatkov in informacij izven Republike Slovenije na podlagi tega zakona ne zadeva subjektov javne uprave, ki izvajajo dejavnosti s področja nacionalne varnosti, 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:

1. Centralni državni informacijsko-komunikacijski sistem je osrednji državni informacijsko-komunikacijsko omrežje oziroma sistem v upravljanju ministrstva, pristojnega za upravljanje informacijsko-komunikacijskih sistemov, namenjeno povezovanju lokalnih omrežij organov državne uprave in drugih subjektov za namene izvrševanja njihovih zakonskih obveznosti ter dostopa do skupnih informacijskih rešitev in informacijsko-komunikacijske infrastrukture preko centraliziranega upravljanja in nadzora.

2. CSIRT je skupina, ki se odziva na incidente na področju računalniške varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov.

3. Digitalna storitev pomeni katero koli storitev informacijske družbe ali katero koli storitev, ki se običajno opravi odplačno, na daljavo, elektronsko in na posamezno zahtevo prejemnika storitev.

4. Dnevniški zapis je zapis dogodkov v omrežnih in informacijskih sistemih, ki omogoča natančen pregled vseh zapisov, povezanih z vsemi dogodki in vsemi shranjenimi informacijami, od nastanka podatka ali informacije naprej do trenutnega stanja.

5. Elektronska komunikacijska storitev pomeni storitev, ki se navadno izvaja za plačilo prek elektronskih komunikacijskih omrežij in ki razen storitev, s katerimi se zagotavljajo vsebine ali izvaja uredniški nadzor nad vsebinami, ki se pošiljajo po elektronskih komunikacijskih omrežjih in z elektronskimi komunikacijskimi storitvami, zajema naslednje storitve:

- storitev dostopa do interneta, pomeni javno dostopno elektronsko komunikacijsko storitev, ki omogoča dostop do interneta in s tem povezljivost s tako rekoč vsemi končnimi točkami interneta, ne glede na uporabljeno omrežno tehnologijo in terminalsko opremo;
- medosebno komunikacijsko storitev in
- storitve, v celoti ali pretežno sestavljene iz prenosa signalov, kot so storitve prenosa, ki se uporabljajo za opravljanje storitev stroj–stroj in za radiodifuzijo.

6. ENISA pomeni Agencijo Evropske unije za kibernetsko varnost.

7. Evropska organizacijska mreža za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe) je skupnost, ki podpira usklajeno obvladovanje kibernetskih incidentov velikih razsežnosti in kriz na operativni ravni in zagotavlja redno izmenjavo relevantnih informacij med državami članicami Evropske unije ter institucijami, organi, uradi in agencijami Evropske unije ter je sestavljena iz predstavnikov organov članic za obvladovanje kibernetskih kriz ter v določenih primerih tudi predstavnikov Evropske komisije, ki sicer sodeluje kot opazovalka.

8. 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.

9. Incident velikih razsežnosti pomeni incident, ki povzroči motnjo, ki presega zmožnost Republike Slovenije za odziv nanj, ali incident, ki pomembno vpliva na vsaj dve državi članici Evropske unije.

10. Informacijska varnost je zaščita, varovanje in obramba omrežnih in informacijskih sistemov pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti.

11. Javno elektronsko komunikacijsko omrežje pomeni elektronsko komunikacijsko omrežje, ki se v celoti ali pretežno uporablja za zagotavljanje javno dostopnih elektronskih komunikacijskih storitev, ki podpirajo prenos informacij med omrežnimi priključnimi točkami.

12. Kibernetska grožnja pomeni vsako potencialno okoliščino, dogodek ali dejanje, ki bi lahko poškodovalo, prekinilo ali drugače škodljivo vplivalo na omrežja in informacijske sisteme, uporabnike takih sistemov in druge osebe.

13. Kibernetska higiena pomeni dobro prakso ohranjanja varnosti in zaščite informacij v digitalnem okolju. To vključuje različne ukrepe in postopke, namenjene zaščiti računalniških sistemov, omrežij ter podatkov pred različnimi varnostnimi grožnjami.

14. Kibernetski incident velikih razsežnosti pomeni incident, ki povzroči motnjo, ki presega zmožnost Republike Slovenije za odziv nanj, ali incident, ki pomembno vpliva na vsaj dve državi članici Evropske unije.

15. Kibernetska obramba je celota ukrepov, dejavnosti in zmogljivosti državnih organov, organov lokalne samouprave, gospodarskih družb, zavodov in drugih organizacij ter državljanov in državljank, ki so potrebne za zaščito kibernetskega prostora, pred kibernetskimi grožnjami in incidenti.

16. Kibernetski prostor je globalno informacijsko okolje, ki ga tvorijo informacijski sistemi in omrežja, podatki, digitalne naprave in njihovi uporabniki.

17. Kibernetska varnost pomeni dejavnosti, ki so potrebne za zaščito omrežnih in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje.

18. Ključni deli nacionalnegavarnostnega sistema so omrežja in informacijski sistemi namenjeni področju obrambe, varstva pred naravnimi in drugimi nesrečami, policije, obveščevalno-varnostne dejavnosti ter zunanjih zadev.

19. Ključni informacijski sistemi so vsi omrežni in informacijski sistemi s pripadajočimi podatki zavezanca, brez katerih ta ne more neprekinjeno izvajati storitev, ki so razvidne iz Priloge I ali II pod vrsto subjekta oziroma storitev, ki bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti.

20. Kratica IKT pomeni informacijska-komunikacijska tehnologija.

21. Kriza pomeni resno grožnjo temeljnim vrednotam in družbenim normam, za katero so značilni časovni pritisk in negotove okoliščine, ki zahtevajo hitro odločanje in izvajanje ukrepov, ki odstopajo od običajnih in predpisanih institucionalnih poti ter zahtevajo uporabo mehanizmov kriznega upravljanja.

22. Krmilni informacijski sistemi so informacijski sistemi, ki omogočajo nadzor, regulacijo, avtomatizacijo ali optimizacijo delovanja ključnih industrijskih, tehnoloških ali infrastrukturnih procesov subjekta.

23. Kvalificirana storitev zaupanja pomeni storitev zaupanja, ki izpolnjuje zadevne zahteve iz zakona, ki ureja elektronsko identifikacijo in storitve zaupanja.

24. Mreža skupin CSIRT je skupnost, ki prispeva h krepitvi zaupanja ter spodbuja hitro in učinkovito operativno sodelovanje med državami članicami Evropske unije, v katero sodelujejo skupine CSIRT iz držav članic in CERT-EU ter Evropska komisija kot opazovalka.

25. Nacionalni center za krizno upravljanje je center, določen v predpisu, ki ureja organizacijo in delovanje nacionalnega centra za krizno upravljanje.

26. Nadzorni informacijski sistemi so informacijski sistemi, preko katerih se izvaja upravljanje in nadzor delovanja omrežij in informacijskih sistemov subjekta, vključno z zaznavanjem in odzivanjem na varnostne dogodke, anomalije in grožnje.

27. Obvladovanje incidentov pomeni vsa dejanja in postopke, namenjene preprečevanju, odkrivanju, analizi in zajezitvi incidentov ali odzivanju nanje in okrevanju po njih.

28. Omrežje za dostavo vsebin pomeni mrežo geografsko porazdeljenih strežnikov za zagotavljanje visoke razpoložljivosti, dostopnosti ali hitre dostave digitalnih vsebin in storitev uporabnikom interneta v imenu ponudnikov vsebin in storitev.

29. Omrežni in informacijski sistem pomeni:
- elektronsko komunikacijsko omrežje, kot je opredeljeno v zakonu, ki ureja elektronske komunikacije;
- vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali
- digitalne podatke, ki jih elementi iz prve in druge alineje shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja.

30. Platforma za storitve družbenega mreženja pomeni platformo, ki končnim uporabnikom omogoča, da se povezujejo, si izmenjujejo vsebine, se spoznavajo in komunicirajo med seboj prek več naprav ter zlasti prek klepetov, objav, videoposnetkov in sporočil.

31. Pomembna kibernetska grožnja pomeni kibernetsko grožnjo, za katero se glede na njene tehnične značilnosti lahko domneva, da bi lahko resno vplivala na omrežne in informacijske sisteme subjekta ali na uporabnike njegovih storitev tako da bi povzročila znatno premoženjsko ali nepremoženjsko škodo.

32. Ponudnik storitev DNS pomeni subjekt, ki opravlja:
- javno dostopne storitve rekurzivnega razreševanja domenskih imen za končne uporabnike interneta ali
- storitve avtoritativnega razreševanja domenskih imen za uporabo s strani tretjih oseb, razen za korenske imenske strežnike.

33. Ponudnik storitev zaupanja pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja, kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja.

34. Ponudnik kvalificiranih storitev zaupanja pomeni ponudnika storitev zaupanja, ki zagotavlja eno ali več kvalificiranih storitev zaupanja in mu nadzorni organ dodeli kvalificirani status.

35. Ponudnik upravljanih storitev pomeni subjekt, ki opravlja storitve v zvezi z namestitvijo, upravljanjem, delovanjem ali vzdrževanjem IKT izdelkov, omrežij, infrastrukture, aplikacij ali katerih koli drugih omrežnih in informacijskih sistemov, in sicer s pomočjo ali aktivnim upravljanjem, ki se izvaja bodisi v prostorih strank bodisi na daljavo.

36. Ponudnik upravljanih varnostnih storitev pomeni ponudnika upravljanih storitev, ki izvaja ali opravlja pomoč za dejavnosti, povezane z obvladovanjem tveganj za kibernetsko varnost.

37. Postopek IKT pomeni sklop dejavnosti, ki se izvaja za zasnovo, razvoj, dobavo ali vzdrževanje proizvoda IKT ali storitve IKT.

38. Povezani subjekt je državni organ, organ lokalne skupnosti, javna agencija ali nosilec javnih pooblastil ter drugi subjekt, ki se povezuje s centralnim državnim informacijsko-komunikacijskim sistemom.

39. Preizkušeni revizor pomeni preizkušenega revizorja informacijskih sistemov, ki je pridobil strokovni naziv pri Slovenskem inštitutu za revizijo in vpisan v njegov register aktivnih preizkušenih revizorjev informacijskih sistemov.

40. Proizvod IKT pomeni element ali skupino elementov omrežja ali informacijskega sistema.

41. Predstavnik iz V. poglavja tega zakona pomeni fizično ali pravno osebo s sedežem v Evropski uniji, ki je izrecno imenovana, da deluje v imenu ponudnika storitev DNS, registra TLD imen, subjekta, ki opravlja storitve registracije domenskih imen, ponudnika storitev računalništva v oblaku, ponudnika storitev podatkovnega centra, ponudnika omrežja za dostavo vsebine, ponudnika upravljanih storitev, ponudnika upravljanih varnostnih storitev ali ponudnika spletne tržnice, spletnega iskalnika ali platforme za storitve družbenega mreženja, ki nima sedeža v Evropski uniji, s katerim lahko pristojni organ ali skupina CSIRT vzpostavi stik namesto s samim subjektom, kar zadeva obveznosti tega subjekta na podlagi tega zakona.

42. Ranljivost pomeni pomanjkljivost, dovzetnost ali napako proizvoda IKT ali storitve IKT, ki jo kibernetska grožnja lahko izkoristi.

43. Raziskovalna organizacija pomeni subjekt, katerega glavni cilj je izvajati uporabne raziskave ali eksperimentalni razvoj z namenom uporabe rezultatov teh raziskav v komercialne namene, vendar ne vključuje izobraževalnih ustanov.

44. Register vrhnjih domenskih imen ali register TLD imen (v nadaljnjem besedilu: register TLD imen) pomeni subjekt, ki mu je bila dodeljena določena vrhnja domena in je odgovoren za njeno upravljanje, vključno z registracijo domenskih imen pod vrhnjo domeno in tehničnim upravljanjem vrhnje domene, vključno z upravljanjem njenih imenskih strežnikov, vzdrževanjem njenih podatkovnih zbirk in porazdelitvijo datotek območij vrhnje domene po imenskih strežnikih, ne glede na to, ali katero od teh dejavnosti subjekt izvaja sam ali jo izvajajo zunanji izvajalci, izključeni pa so primeri, v katerih register TLD imen uporablja vrhnja domenska imena zgolj za lastne potrebe.

45. Revizijska sled je nespremenljiva sled oziroma niz podatkov o dogodku, ki se je zgodil v informacijskem sistemu ali napravi, z natančnim časovnim zapisom.

46. Semaforski protokol je skupek pravil in dogovorov o omejitvah v zvezi z nadaljnjim širjenjem prejetih ali deljenih informacij, kot ga uporabljajo pri izmenjavi informacij skupine CSIRT.

47. Sistem domenskih imen ali DNS pomeni hierarhično porazdeljen sistem poimenovanja, ki omogoča identifikacijo internetnih storitev in virov ter napravam končnih uporabnikov omogoča, da z uporabo internetnih storitev usmerjanja in povezljivosti dostopajo do teh storitev in virov.

48. Skupina za sodelovanje je skupina, ki podpira in olajšuje strateško sodelovanje in izmenjavo informacij med državami članicami Evropske unije ter krepi zaupanje med njimi in jo sestavljajo predstavniki držav članic Evropske unije, Evropske komisije in ENISA ter Evropska služba za zunanje delovanje kot opazovalka.

49. Skorajšnji incident pomeni dogodek, ki bi lahko ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih

omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni, vendar se je uspešno preprečilo, da bi se ta dogodek uresničil, ali se ni uresničil.

50. Spletni iskalnik pomeni digitalno storitev, ki uporabnikom omogoča vnos poizvedb za izvedbo iskanja po vseh spletiščih ali vseh spletiščih v določenem jeziku, na podlagi poizvedbe na katero koli temo v obliki ključne besede, glasovne zahteve, fraze ali drugega vnosa, poda pa rezultate v katerem koli formatu z informacijami o zahtevani vsebini.

51. Spletna tržnica pomeni storitev, ki uporablja programsko opremo, vključno s spletno stranjo, delom spletne strani ali aplikacije, ki jo upravlja trgovec ali nekdo v njegovem imenu, ki potrošnikom omogočajo, da sklepajo pogodbe na daljavo z drugimi trgovci ali potrošniki.

52. Standard pomeni tehnično specifikacijo, ki jo je sprejel priznan organ za standardizacijo za večkratno ali stalno uporabo, skladnost s katero ni obvezna in sodi v eno od naslednjih kategorij:

- mednarodni standard pomeni standard, ki ga je sprejel mednarodni organ za standardizacijo;
- evropski standard pomeni standard, ki ga je sprejela evropska organizacija za standardizacijo;
- harmonizirani standard pomeni evropski standard, sprejet na podlagi zahteve Evropske komisije za uporabo usklajevalne zakonodaje Evropske unije;
- nacionalni standard pomeni standard, ki ga je sprejel nacionalni organ za standardizacijo.

53. Stičišče omrežij pomeni omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih omrežij (avtonomnih sistemov), predvsem zaradi izmenjave internetnega prometa, ki zagotavlja medsebojno povezavo zgolj avtonomnim sistemom in ki ne zahteva, da izmenjava internetnega prometa med katerima koli sodelujočima avtonomnima sistemoma prehaja prek tretjega avtonomnega sistema, in ne spreminja takšnega prometa ali kako drugače posega vanj.

54. Storitev IKT pomeni storitev, ki v celoti ali pretežno sestoji iz prenosa, shranjevanja, priklica ali obdelave informacij prek omrežij in informacijskih sistemov.

55. Storitev podatkovnega centra pomeni storitev, ki vključuje strukture ali skupine struktur, namenjene centralizirani namestitvi, medsebojnemu povezovanju in delovanju opreme za informacijsko tehnologijo in omrežne opreme za storitve shranjevanja, obdelave in prenosa podatkov vključno z vsemi zmogljivostmi in infrastrukturami za zagotavljanje električne energije in nadzor okoljski razmer v podatkovnem centru.

56. Storitev v oblaku pomeni digitalno storitev, ki omogoča upravljanje na zahtevo in širok oddaljeni dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov, tudi kadar so ti viri porazdeljeni na več lokacijah.

57. Storitev zaupanja pomeni elektronsko storitev, ki se praviloma opravlja za plačilo in vključuje:

- ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, ali
- ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali
- hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami.

58. Strategija kibernetske varnosti pomeni okvir, ki določa strateške cilje in prednostne naloge na področju kibernetske varnosti ter upravljanja za njihovo uresničitev v Republiki Sloveniji.

59. Subjekt, ki opravlja storitve registracije domenskih imen pomeni registrarja ali zastopnika, ki deluje v imenu registrarja, kot je ponudnik storitev registracije za zasebnost ali pooblaščenec ali preprodajalec.

60. Subjekt javne uprave pomeni organ državne uprave ali organ lokalne samouprave, ali javni infrastrukturni zavod ustanovljen v skladu z zakonom, ki ureja znanstveno raziskovalno in inovacijsko dejavnost . Pomeni pa tudi tisti drug subjekt, ki je v Republiki Sloveniji priznan kot samostojna oseba javnega prava, razen pravosodnega sistema, Državnega zbora Republike Slovenije, Državnega sveta Republike Slovenije in Banke Slovenije, in ki izpolnjuje naslednja merila:

- je ustanovljen za izpolnitev potreb v splošnem interesu in ni industrijske ali komercialne narave;
- je pravna oseba ali ima po zakonu pravico delovati v imenu drugega subjekta, ki je pravna oseba;
- pretežno ga financirajo država, regionalni organi ali druge osebe javnega prava, njegovo upravljanje nadzorujejo ti organi ali osebe ali pa ima upravni, upraviteljski ali nadzorni odbor, v katerega več kot polovico članov imenujejo država, regionalni organi ali druge osebe javnega prava;
- ima pooblastilo, da na fizične ali pravne osebe naslovi upravne ali regulativne odločbe, ki vplivajo na njihove pravice.

61. Subjekt pomeni fizično ali pravno osebo, ki je ustanovljena in priznana kot taka po nacionalnem pravu njenega kraja sedeža ter lahko v svojem imenu uveljavlja pravice in prevzema obveznosti.

62. Tehnična specifikacija pomeni tehnično specifikacijo na področju informacijske in komunikacijske tehnologije.

63. Tretja država pomeni državo, ki ni članica Evropske unije ali državo, ki ni podpisnica Sporazuma o ustanovitvi Evropskega gospodarskega prostora (UL L št. 1 z dne 3. 1. 1994, str. 3).

64. Tveganje pomeni možnost izgube ali motnje zaradi incidenta ter je izraženo kot kombinacija razsežnosti izgube ali motnje in verjetnosti, da bi do incidenta prišlo.

65. Varnostni pregled je postopek, v katerem inšpektor pri zavezancu v postopku inšpekcijskega nadzora izvede identifikacijo in oceno morebitnih ranljivosti v omrežnih in informacijskih sistemih, izvede preizkus učinkovitosti varnostnih ukrepov oziroma mehanizmov in izpostavljenosti kibernetskim grožnjam ter preveri ustreznost izvajanja učinkovitega zaznavanja in obravnavanja kibernetskih incidentov.

66. Varnost omrežnih in informacijskih sistemov pomeni zmožnost omrežnih in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vsak dogodek, ki lahko ogrozi 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.

67. Varnostno operativni center organa državne uprave je notranja organizacijska enota posameznega organa državne uprave, ki se odziva na incidente na področju informacijske varnosti in izpolnjuje pogoje zanj iz tega zakona.

68. Varovani podatek pristojnega nacionalnega organa je podatek o ranljivostih ali stanju informacijskih sistemov in omrežij zavezancev ter njihova identiteta, 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.

69. Veščak za informacijsko varnost pomeni posameznika ali organizacijo, ki ima izkazano poglobljeno znanje na področju informacijsko komunikacijskih tehnologij katerega ali katere delo revizor uporabi kot pomoč revizorju pri pridobivanju zadostnih in ustreznih revizijskih dokazov.

II. Zavezanci

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 ali letno bilančno vsoto vsaj 43 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;

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 – ZDU-1O in 49/23) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023;

8. subjekti iz sektorja 9. Upravljanje storitev IKT Priloga I in niso subjekti iz točk 1 do 7 tega odstavka, ki jih na podlagi poimenskega seznama, ki ga pristojni organi po zakonu, ki ureja izvajanje Uredbe (EU) 2022/2554, posredujejo pristojnemu nacionalnemu organu, določi vlada.

(3) Za namene tega zakona se šteje, da so pomembni subjekti:

- subjekti vrste iz Prilog I ali II vključno s tistimi, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada z odločbo in
- drugi subjekti oziroma organi iz 3. člena tega zakona,

ki se ne štejejo za bistvene subjekte na podlagi prejšnjega odstavka.

(4) Ne glede na določbo 7. točke drugega odstavka tega člena Banka Slovenije ni zavezanec po tem zakonu.

(5) Določbe prvega, drugega in tretjega odstavka tega člena ne veljajo za druge fizične in pravne osebe iz dvanajstega odstavka 3. člena tega zakona, ki se za njih uporablja v delu, ki ureja certifikacijski okvir za kibernetsko varnost.

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 v desetih delovnih dneh od dneva, ko so nastopile okoliščine, na podlagi katerih izpolnjujejo merila iz prejšnjega člena. Ob tem podajo 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;
- 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 desetih delovnih dneh od datuma spremembe. V primeru, da subjekt, ki se je samoregistriral na podlagi prejšnjega odstavka ugotovi, da ne spada več med zavezance iz prejšnjega člena tega zakona, o tem in razlogih za takšno ugotovitev obvesti pristojni nacionalni organ, ki preveri navedbe in ob potrditvi razlogov v mehanizem za samoregistracijo vnese podatek o takšni spremembi.

(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, ki je varovani podatek pristojnega nacionalnega organa, pristojni nacionalni organ redno oziroma vsaj vsaki dve leti pregleda in po potrebi posodobi.

(5) Do seznama iz prejšnjega odstavka imajo v delu, ki se nanaša na zavezance iz njihove pristojnosti, dostop tudi pristojne skupine CSIRT.

(6) Pristojni nacionalni organ obvesti Evropsko komisijo in Skupino za sodelovanje o številu bistvenih in pomembnih subjektov, ki so na seznamu iz četrtega odstavka tega člena za vsak sektor in podsektor iz Priloge I ali II.

(7) Pristojni nacionalni organ Evropsko komisijo obvesti o ustreznih informacijah o številu bistvenih in pomembnih subjektov ne glede na njihovo velikost, identificiranih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona. Ob tem za vsakega zavezanca navede tudi sektor in podsektor iz Priloge I ali II, v katerega sodijo in vrsto storitev, ki jih opravljajo. Izmed 2. do 5. točke drugega odstavka 3. člena tega zakona se ob tem navede tudi konkretno določbo na podlagi katere so bili zadevni subjekti identificirani. Pristojni nacionalni organ lahko Evropski komisiji na njeno zahtevo uradno sporoči tudi imena bistvenih in pomembnih subjektov.

(8) Obveščanje iz prejšnjega in šestega odstavka tega člena pristojni nacionalni organ izvaja vsaki dve leti.

(9) Organi, ki so pristojni za izvajanje področnih predpisov iz devetega odstavka 3. člena tega zakona, 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.

III. Organizacija nacionalnega sistema informacijske varnosti

8. člen
(strategija kibernetske varnosti)

(1)Vlada sprejme strategijo kibernetske varnosti (v nadaljnjem besedilu: strategija), ki predstavlja okvir za izvedbo ukrepov za vzpostavitev učinkovitega nacionalnega sistema zagotavljanja informacijske oziroma kibernetske varnosti. V strategiji so opredeljeni strateški cilji, potrebna sredstva za dosego teh ciljev ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetske varnosti na področju uporabe tega zakona.
V strategijo se vključijo zlasti:

1. cilje in prednostne naloge strategije;
2. okvir upravljanja za dosego ciljev in izvedbo prednostnih nalog iz prejšnje točke, vključno s politikami iz naslednjega odstavka tega člena;
3. okvir upravljanja, ki opredeljuje vloge in odgovornosti ustreznih zainteresiranih deležnikov kibernetske varnosti na državni ravni ter podpira sodelovanje in usklajevanje na državni ravni med pristojnim nacionalnim organom, enotno kontaktno točko in skupinami CSIRT iz tega zakona, pa tudi usklajevanje in sodelovanje med temi organi in pristojnimi organi na podlagi področnih pravnih aktov Evropske unije oziroma področne zakonodaje, ki te akte prenaša v slovenski pravni red;
4. mehanizem za opredelitev ustreznih virov in oceno tveganj;
5. opredelitev ukrepov za zagotovitev pripravljenosti na odzivanja na incidente in okrevanja po njih, vključno s sodelovanjem med javnim in zasebnim sektorjem;
6. seznam organov, organizacij in deležnikov, vključenih v izvajanje strategije;
7. okvir politike za okrepljeno usklajevanje med pristojnimi nacionalnimi organi iz tega zakona in pristojnim nacionalnim organom iz zakona, ki ureja kritično

infrastrukturo za namene izmenjave informacij o tveganjih, kibernetskih grožnjah in incidentih ter o nekibernetskih tveganjih, grožnjah in incidentih ter izvajanju nadzornih nalog, kot je ustrezno;
8. načrt, vključno s potrebnimi ukrepi, za povečanje splošne ozaveščenosti državljanov o kibernetski varnosti.

(2) Strategija vključuje zlasti naslednje politike:
1. obravnavanja kibernetske varnosti v dobavni verigi proizvodov IKT in storitev IKT, ki jih subjekti uporabljajo za opravljanje svojih storitev;
2. o vključitvi in specifikaciji zahtev za proizvode IKT in storitve IKT pri javnem naročanju, povezanih s kibernetsko varnostjo, vključno v zvezi s certificiranjem kibernetske varnosti, šifriranjem in uporabo odprtokodnih proizvodov za kibernetsko varnost;
3. obvladovanja ranljivosti, vključno s spodbujanjem in omogočanjem usklajenega razkrivanja ranljivosti na podlagi prvega odstavka 16. člena tega zakona;
4. povezane z ohranjanjem splošne razpoložljivosti, celovitosti in zaupnosti javnega jedra odprtega interneta, vključno, kadar je to ustrezno, s kibernetsko varnostjo podmorskih komunikacijskih kablov;
5. spodbujanja razvoja in vključevanja ustreznih naprednih tehnologij za izvajanje najsodobnejših ukrepov za obvladovanje tveganj na področju kibernetske varnosti;
6. spodbujanja in razvoja izobraževanja in usposabljanja na področju kibernetske varnosti, spretnosti na področju kibernetske varnosti, dviganja ozaveščanja ter raziskovalnih in razvojnih pobud na področju kibernetske varnosti ter smernic o dobrih praksah in nadzoru kibernetske higiene, namenjenih državljanom, deležnikom in subjektom;
7. podpiranja akademskih in raziskovalnih institucij pri razvoju, izboljševanju in spodbujanju uvajanja orodij kibernetske varnosti in varne omrežne infrastrukture;
8. vključevanja ustreznih postopkov in primernih orodij za izmenjavo informacij za podpiranje prostovoljne izmenjave informacij o kibernetski varnosti med subjekti v skladu s pravom Evropske unije;
9. krepitve kibernetske odpornosti in osnovne kibernetske higiene malih in srednjih podjetij, zlasti tistih, ki so izključena s področja uporabe tega zakona, z zagotavljanjem lahko dostopnih smernic in pomoči za njihove posebne potrebe;
10. spodbujanja aktivne kibernetske zaščite.

(3) Pristojni nacionalni organ v treh mesecih od sprejeta strategije iz tega člena o tem uradno obvesti Evropsko komisijo. Pri tem lahko izključi informacije, ki so pomembne za nacionalno varnost.

(4) Pristojni nacionalni organ redno in vsaj vsakih pet let oceni strategijo na podlagi ključnih kazalnikov uspešnosti in po potrebi predlaga vladi njeno posodobitev.

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:
1. koordinira delovanje nacionalnega sistema informacijske varnosti;

2. razvija zmogljivosti za izvajanje kibernetske obrambe;
3. vsem zavezancem pri izvajanju njihovih nalog nudi strokovno podporo na področju informacijske varnosti;
4. zagotavlja analize, metodološko podporo in preventivno delovanje na področju informacijske varnosti ter daje mnenja s področja svojih pristojnosti;
5. sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, predvsem s skupinami CSIRT, z varnostno operativnimi centri organov državne uprave, z regulatorji oziroma nadzorniki področij iz Prilog I in II, z Informacijskim pooblaščencem in z organi kazenskega pregona ter s ponudniki varnostnih rešitev;
6. zavezance ozavešča o pomembnosti prijave incidenta z vsemi znaki kaznivega dejanja, ki se preganja po uradni dolžnosti, organom kazenskega pregona, skladno s Kazenskim zakonikom;
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;
8. spodbuja in podpira raziskave in razvoj na področju informacijske varnosti;
9. skrbi za pripravo in izvajanje strategije;
10. izdela in vzdržuje nacionalni načrt odzivanja na kibernetske incidente, kibernetske incidente velikih razsežnosti in krize ob upoštevanju strategije, načrtov skupin CSIRT, drugih pristojnih organov ter varnostne dokumentacije zavezancev;
11. pregleduje ustreznost določitve zavezancev iz 5. točke, drugega odstavka 6. člena tega zakona vsaj vsaki dve leti ter vladi lahko predlaga posodobitev seznama zavezancev;
12. za statistične namene in namene seznanjanja javnosti dvakrat letno pripravi anonimizirane informacije o priglašenih incidentih, ki jih javno objavi na svoji spletni strani;
13. je član Skupine za sodelovanje, v katero imenuje svoje predstavnike in zagotovi njihovo učinkovito in uspešno delovanje;
14. imenuje predstavnike v Evropsko mrežo organizacij za zvezo za kibernetske krize;
15. sodeluje pri aktivaciji nudenja in sprejemanja pomoči za obvladovanje kibernetskih kriz v skladu z mednarodnimi pogodbami in dogovori;
16. imenuje predstavnika v upravni odbor Agencije Evropske unije za kibernetsko varnost (ENISA) in sodeluje pri delu omenjene agencije;
17. izpolnjuje druge obveznosti iz neposredno uporabljivih aktov Evropske unije s področja kibernetske varnosti;
18. izpolnjuje druge obveznosti obveščanja Evropske komisije in Skupine za sodelovanje, obveznosti obveščanja in notifikacije preostalih mednarodnih organizacij;
19. vodi koordinacijsko delovno skupino za mednarodno sodelovanje na področju kibernetske varnosti;
20. izvaja druge naloge mednarodnega sodelovanja;
21. pripravlja predloge predpisov s področja informacijske in kibernetske varnosti;
22. izvaja naloge nacionalnega certifikacijskega organa za kibernetsko varnost;
23. odloča o sodelovanju pri medsebojnih strokovnih pregledih.

(3) Pristojni nacionalni organ o njegovi določitvi ter nalogah in vsakokratnih spremembah pri tem brez nepotrebnega odlašanja uradno obvesti Evropsko komisijo.

10. člen
(enotna kontaktna točka)

(1) Za enotno kontaktno točko po tem zakonu je določen pristojni nacionalni organ.

(2) Enotna kontaktna točka ima povezovalno vlogo in zagotavlja čezmejno sodelovanje z ustreznimi organi drugih držav članic Evropske unije in, kadar je to ustrezno, Evropsko komisijo in ENISA.

(3) Pristojni nacionalni organ o določitvi enotne kontaktne točke ter njenih nalogah in ob vsakokratnih spremembah o tem brez nepotrebnega odlašanja uradno obvesti Evropsko komisijo.

11. člen
(nacionalni okvir za obvladovanje kibernetskih kriz)

(1) Pristojni organ za obvladovanje kibernetskih incidentov velikih razsežnosti in kibernetskih kriz (v nadaljnjem besedilu: organ za obvladovanje kibernetskih kriz) v Republiki Sloveniji je Urad Vlade Republike Slovenije za informacijsko varnost, ki sodeluje v Evropski mreži organizacij za zvezo za kibernetske krize (v nadaljnjem besedilu: mreža EU-CyCLONe).

(2) Organ za obvladovanje kibernetskih kriz izdela nacionalni načrt odzivanja na kibernetske incidente, kibernetske incidente velikih razsežnosti in krize (v nadaljnjem besedilu: nacionalni načrt odzivanja), ob upoštevanju strategije, načrtov skupin CSIRT, drugih pristojnih organov ter varnostne dokumentacije zavezancev.

(3) Vlada sprejme nacionalni načrt odzivanja, v katerem so opredeljeni cilji in ureditve obvladovanja kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti in kibernetskih kriz. V tem načrtu se zlasti določijo:

1. cilji nacionalnih ukrepov in dejavnosti za pripravljenost;
2. naloge in odgovornosti organov za obvladovanje kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti in kibernetskih kriz;
3. postopki za obvladovanje kibernetskih incidentov in kibernetskih incidentov velikih razsežnosti;
4. postopki za obvladovanje kibernetskih kriz na način, da se upošteva predpis s področja kriznega upravljanja in vodenja kriz;
5. ukrepi za pripravljenost, vključno z vajami in dejavnostmi usposabljanja;
6. ustrezni javni in zasebni deležniki ter vključena infrastruktura;
7. postopki sodelovanja med organom za obvladovanje kibernetskih kriz in organi iz predpisa s področja kriznega upravljanja in vodenja kriz, z namenom učinkovitega sodelovanja Republike Slovenije ter njene podpore pri usklajenem obvladovanju kibernetskih incidentov velikih razsežnosti in kriz na ravni Evropske unije.

(4) Organ za obvladovanje kibernetskih kriz ob zaznavi kibernetskih incidentov, za katere ocenjuje, da lahko povzročijo kibernetsko krizo nemudoma seznani Svet za nacionalno varnost (v nadaljnjem besedilu: SNAV). V sodelovanju s prizadetimi zavezanci po tem zakonu, pristojnimi področnimi regulatorji ter nosilci sektorjev prizadete kritične infrastrukture organ za obvladovanje kibernetskih kriz analizira stanje ter o ugotovitvah seznanja SNAV in mu po potrebi predlaga ukrepe. SNAV na podlagi predpisov s področja kriznega upravljanja in vodenja kriz izdela oceno situacije. Na podlagi ocene svetuje vladi o nadaljnjih ukrepih

(5) Vlada na predlog SNAV lahko sprejme odločitev o vključitvi drugih državnih zmogljivosti v obvladovanje krize, razglasi krizo ter po potrebi sprejme odločitev o izvajanju kriznega upravljanja in vodenja v kompleksni krizi.

(6)Pristojni nacionalni organ o imenovanju organa za obvladovanje kibernetskih kriz in ob vsakokratnih spremembah o tem uradno obvesti Evropsko komisijo. Evropski komisiji in mreži EU-CyCLONe predloži ustrezne informacije o sprejetju nacionalnega načrta odzivanja v zvezi z zahtevami iz tretjega odstavka tega člena. Iz posredovanja se izključijo informacije katerih razkritje bi bilo v nasprotju z interesi nacionalne varnosti, javne varnosti ali obrambe Republike Slovenije.

(7) Če je v zvezi z izvajanjem tega člena potrebno tudi obveščanje javnosti, pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, pripravi sporočilo za javno objavo, ki ga mediji smejo objaviti le v nespremenjeni obliki.

12. člen
(skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT))

(1) Skupini CSIRT za namene tega zakona sta:
- CSIRT SI-CERT, ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije in
- CSIRT državne uprave, ki deluje kot notranja organizacijska enota SIGOV-CERT pri pristojnem nacionalnem organu.

(2) CSIRT državne uprave je pristojen za obravnavo incidentov subjektov javne uprave na državni in regionalni ravni in ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave.

(3) CSIRT SI-CERT je pristojen za obravnavo incidentov, ki jih priglasijo ostali zavezanci iz prvega odstavka 6. člena tega zakona, subjekti lokalne samouprave in sicer mestne občine in občine, ki imajo sedeže v krajih, kjer so sedeži upravnih enot.

(4) Skupine CSIRT morajo izpolnjevati zahteve iz naslednjega člena ter so pristojne za obvladovanje incidentov v skladu s postopkom določenim s tem zakonom.

(5) Skupine CSIRT izmenjujejo informacije z bistvenimi in pomembnimi subjekti ter drugimi ustreznimi deležniki prek ustrezne, varne in odporne komunikacijske in informacijske infrastrukture, ki jo vzpostavi pristojni nacionalni organ in sodelujejo z njim pri uvajanju in uporabi orodij za varno izmenjavo informacij.

(6) Skupine CSIRT medsebojno sodelujejo in si, kadar je ustrezno, v skladu s 30. členom tega zakona izmenjujejo ustrezne informacije s sektorskimi ali medsektorskimi skupnostmi zavezancev.

(7) Skupine CSIRT sodelujejo pri medsebojnih strokovnih pregledih v skladu z 18. členom tega zakona.

(8) Skupine CSIRT sodelujejo na učinkovit, uspešen in varen način v mreži skupin CSIRT lahko pa tudi v mrežah za mednarodno sodelovanje na enak način.

(9) Skupine CSIRT lahko sodelujejo z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz tretjih držav. Pri tem s temi nacionalnimi skupinami za odzivanje na računalniške varnostne incidente iz tretjih držav lahko izmenjujejo informacije z uporabo ustreznih protokolov, vključno s semaforskim protokolom, z namenom da se zagotovi uspešen, učinkovit in varen način izmenjave informacij. Skupine CSIRT si lahko izmenjujejo ustrezne informacije z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz tretjih držav, vključno z osebnimi podatki v skladu s pravom Evropske unije o varstvu podatkov.

(10) Skupine CSIRT lahko sodelujejo z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz tretjih držav ali enakovrednimi organi tretjih držav, zlasti za zagotavljanje pomoči na področju kibernetske varnosti.

(11) Pristojni nacionalni organ o identiteti skupin CSIRT iz prvega odstavka tega člena ter pristojnosti iz drugega in tretjega odstavka tega člena in vsakokratnih spremembah identitet in pristojnosti glede bistvenih in pomembnih subjektov brez nepotrebnega odlašanja obvesti Evropsko komisijo. Prav tako pristojni nacionalni organ obvesti Evropsko komisijo tudi o identiteti skupine CSIRT, ki je imenovana za koordinatorja iz prvega odstavka 16. člena tega zakona.

13. člen
(zahteve in tehnične zmogljivosti skupin CSIRT)

Skupine CSIRT iz prvega odstavka prejšnjega člena morajo izpolnjevati naslednje zahteve:

1. zagotavljanje visoke stopnje razpoložljivosti svojih komunikacijskih kanalov, tako da preprečujejo posamezne točke odpovedi, in imajo na voljo več načinov, na katere se drugi lahko kadar koli obrnejo nanje in one obrnejo na druge; jasno opredelijo komunikacijske kanale ter o njih obvestijo uporabnike in partnerje;
2. prostori in podporni informacijski sistemi se nahajajo na varnih krajih;
3. imajo ustrezen sistem za upravljanje in usmerjanje zahtevkov, zlasti da se poenostavi njihova učinkovita in uspešna predaja;
4. zagotovijo zaupnost in zanesljivost svojih dejavnosti;
5. imajo dovolj osebja za zagotavljanje neprekinjene razpoložljivosti storitev, pri čemer zagotavljajo, da je to osebje ustrezno usposobljeno;
6. imajo redundantne sisteme in nadomestni delovni prostor, da se zagotovi neprekinjeno izvajanje njihovih storitev.

14. člen
(naloge skupin CSIRT)

(1) Skupine CSIRT iz prvega odstavka 12. člena tega zakona na področjih za katera so pristojne skladno z drugim ali tretjim odstavkom 12. člena tega zakona izvajajo naslednje naloge:

1. spremljanje in analiziranje kibernetskih groženj, ranljivosti in incidentov na državni ravni ter, na zahtevo, pomoč zadevnim bistvenim in pomembnim subjektom v zvezi s spremljanjem njihovih omrežnih in informacijskih sistemov v realnem času ali v skoraj realnem času;
2. zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o kibernetskih grožnjah, ranljivostih in incidentih zadevnim bistvenim in pomembnim subjektom ter pristojnim organom in drugim ustreznim deležnikom, če je mogoče v skoraj realnem času;

3. odzivanje na incidente in zagotavljanje pomoči zadevnim bistvenim in pomembnim subjektom, kadar je to potrebno;
4. zbiranje in analiziranje forenzičnih podatkov in opravljanje dinamičnih analiz tveganja in incidentov ter situacijsko zavedanje na področju kibernetske varnosti;
5. opravljanje, na zahtevo bistvenega ali pomembnega subjekta, proaktivnega pregleda omrežnih in informacijskih sistemov zadevnega subjekta, da se odkrijejo ranljivosti, ki bi lahko imele pomemben vpliv;
6. sodelovanje v mreži skupin CSIRT in zagotavljanje medsebojne pomoči v skladu z zmožnostmi in pristojnostmi drugim članicam mreže skupin CSIRT na njihovo zahtevo;
7. prispevanje k uporabi orodij za varno izmenjavo informacij na podlagi petega odstavka 12. člena tega zakona.
8. medsebojno pomoč in sodelovanje z drugimi organi, ki so na podlagi predpisov pristojni za obravnavanje incidentov.

(2) Skupine CSIRT iz prvega odstavka 12. člena tega zakona lahko izvajajo proaktivno in nevsiljivo pregledovanje javno dostopnih omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov, za katere so pristojne skladno z drugim ali tretjim ali četrtim odstavkom 12. člena tega zakona. Takšno pregledovanje se izvaja z namenom odkrivanja ranljivosti omrežnih in informacijskih sistemov, ki niso konfigurirani na varen način ter za obveščanje zadevnih subjektov s ciljem odpravljanja varnostnih groženj. Takšno pregledovanje ne sme negativno vplivati na delovanje storitev teh subjektov.

(3) Skupine CSIRT iz prvega odstavka 12. člena tega zakona lahko pri izvajanju nalog iz prvega odstavka tega člena prednostno razvrstijo nekatere naloge na podlagi pristopa, ki temelji na tveganjih.

(4) Skupine CSIRT pristojnemu nacionalnemu organu posredujejo tedensko in četrtletno poročilo o izvajanju svojih nalog, v katerega vključijo informacije o vseh priglašenih incidentih, ki so jih obravnavale

(5) Skupine CSIRT nemudoma obvestijo pristojni nacionalni organ o lastnem incidentu, ki bi lahko vplival ali vpliva na delovanje in razpoložljivost njihovih storitev, ki jih nudijo zavezancem in prostovoljnim priglasiteljem.

(6) V skladu z usmeritvami pristojnega nacionalnega organa skupina CSIRT v primeru razglasitve ocene ogroženosti visoko ali kritično izda varnostno obvestilo ali navodilo v skladu s petim in šestim odstavkom 33. člena tega zakona.

(7) Skupina CSIRT pristojna za državno upravo je, za namen učinkovitega izvajanja nalog informacijske in kibernetske varnosti ter kibernetske obrambe, pooblaščena za neposredni, nujni in sorazmerni vpogled v delovanje informacijske infrastrukture centralnega informacijsko-komunikacijskega sistema. Upravljavec centralnega informacijsko-komunikacijskega sistema mu mora to omogočiti.

(8) Za namen pravočasnega odzivanja na kibernetske grožnje in preprečevanja škodljivih posledic morebitnega težjega ali kritičnega incidenta ter zaradi izvajanja kibernetske obrambe je skupina CSIRT pristojna za državno upravo pooblaščena, da upravljavcu centralnega informacijsko-komunikacijskega sistema odredi ustrezne, nujne in sorazmerne ukrepe, ki jih mora ta nemudoma oziroma v postavljenem roku izvesti v svojem informacijsko-komunikacijskem sistemu.

(9) Skupine CSIRT iz prvega odstavka 12. člena tega zakona lahko izvajajo tudi programe ozaveščanja v skladu s Strategijo kibernetske varnosti.

15. člen
(sodelovanje skupin CSIRT z deležniki zasebnega sektorja)

(1) Skupine CSIRT iz prvega odstavka 12. člena tega zakona za dosego ciljev tega zakona vzpostavijo sodelovanje z ustreznimi deležniki iz zasebnega sektorja.

(2) Za olajšanje sodelovanja iz prejšnjega odstavka skupine CSIRT spodbujajo 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.

16. člen
(usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti)

(1) CSIRT SI-CERT je koordinator za usklajeno razkrivanje ranljivosti v Republiki Sloveniji (v nadaljnjem besedilu koordinator), ki deluje kot zaupanja vreden posrednik in po potrebi olajšuje sodelovanje med fizično ali pravno osebo, ki poroča o ranljivostih, in proizvajalcem ali ponudnikom proizvodov IKT ali storitev IKT, ki naj bi zajemali ranljivost, in sicer na pobudo katere koli stranke.

(1)Naloge koordinatorja vključujejo:

- identifikacijo zadevnih subjektov in vzpostavitev stika z njimi;
- podpiranje fizičnih ali pravnih oseb, ki poročajo o ranljivosti, in
- pogajanja o časovnicah razkrivanja in obvladovanju ranljivosti, ki vplivajo na več subjektov.

(2)Fizične ali pravne osebe iz prvega odstavka tega člena lahko koordinatorju o ranljivostih poročajo anonimno. Koordinator zagotovi skrbno nadaljnje ukrepanje v zvezi s sporočenimi ranljivostmi in anonimnost fizične ali pravne osebe, ki je o ranljivosti poročala. Kadar bi lahko sporočena ranljivost pomembno vplivala na subjekte tudi v drugih državah članicah Evropske unije, koordinator po potrebi sodeluje z drugimi skupinami CSIRT, ki so imenovane za koordinatorke v okviru mreže skupin CSIRT.

(3)Koordinator v zvezi s sporočenimi ranljivostmi sodeluje tudi z ENISA, ki vodi evropsko podatkovno zbirko ranljivosti, v skladu z Aktom Evropske unije o kibernetski odpornosti.

(6) Koordinator pristojnemu nacionalnemu organu posreduje tedensko poročilo o izvajanju svojih nalog iz tega člena, v katerega vključi informacije o vseh zaznanih ranljivostih iz prvega odstavka tega člena.

(7) Če je ranljivost prisotna v sistemih zavezancev po tem zakonu, koordinator, nemudoma obvesti pristojni nacionalni organ. Pri temu mu posreduje

- informacije, ki opisujejo ranljivost;

- prizadeti proizvodi IKT ali storitve IKT ter resnost ranljivosti v smislu okoliščin, v katerih jo je mogoče izkoristiti;
- razpoložljivost povezanih popravkov ter, če popravki niso na voljo, smernice, ki jih določi koordinator, naslovljene na uporabnike proizvodov IKT in storitev IKT z ranljivostmi, o načinih za zmanjšanje tveganj, ki izhajajo iz razkritih ranljivosti

(7) Koordinator v posvetovanju s pristojnim nacionalnim organom na podlagi podatkov in informacij iz prejšnjega odstavka vzpostavi in vodi nacionalno podatkovno zbirko ranljivosti in vzdržuje ustrezne informacijske sisteme, politike in postopke ter sprejme potrebne tehnične in organizacijske ukrepe, s katerimi zagotovi varnost in celovitost te zbirke.

(8) Do podatkovne zbirke iz prejšnjega odstavka imajo dostop pristojni nacionalni organ, skupine CSIRT in zavezanci na podlagi tega zakona.

17. člen
(sodelovanje na nacionalni ravni)

(1)Za zagotovitev učinkovitega opravljanja nalog in obveznosti pristojnega nacionalnega organa, enotne kontaktne točke in skupin CSIRT iz tega zakona se vzpostavi ustrezno sodelovanje na nacionalni ravni na način, da ti subjekti:

1. medsebojno sodelujejo pri izpolnjevanju obveznosti;
2. sodelujejo z organi kazenskega pregona, Informacijskim pooblaščencem, Javno agencijo za civilno letalstvo Republike Slovenije, Inšpekcijo za informacijsko družbo, Banko Slovenije, Agencijo za komunikacijska omrežja in storitve Republike Slovenije in pristojnim nacionalnim organom iz zakona, ki ureja kritično infrastrukturo ter pristojnimi organi oziroma sektorskimi regulatorji iz drugih področnih zakonov iz področij, ki jim pripadajo zavezanci iz 6. člena tega zakona;
3. redno sodelujejo s pristojnim nacionalnim organom iz zakona, ki ureja kritično infrastrukturo in si izmenjujejo informacije o identifikaciji kritičnih subjektov, o tveganjih, kibernetskih grožnjah in incidentih, pa tudi o nekibernetskih tveganjih, grožnjah in incidentih, ki vplivajo na bistvene subjekte, ki so opredeljeni kot kritični subjekti na podlagi zakona, ki ureja kritično infrastrukturo, ter o ukrepih, sprejetih v odziv na takšna tveganja, grožnje in incidente;
4. redno izmenjujejo informacije, tudi o relevantnih incidentih in kibernetskih grožnjah z Inšpekcijo za informacijsko družbo, Banko Slovenije, Javno agencijo za civilno letalstvo Republike Slovenije in Agencijo za komunikacijska omrežja in storitve Republike Slovenije.

(2) Medsebojna izmenjava informacij o incidentih, kibernetskih grožnjah in skorajšnjih incidentih iz členov 25. in 31. tega zakona s strani organov iz prvega odstavka tega člena in pristojnih organov iz 3. in 4. točke prejšnjega odstavka se izvaja z uporabo digitalne platforme, ki jo vzpostavi pristojni nacionalni organ. Do vzpostavitve navedene platforme se zagotovi varnost prenesenih podatkov po elektronski poti, če je to le mogoče.

(3) Za potrebe nacionalnega sistema za zagotavljanje informacijske varnosti lahko pristojni nacionalni organ in skupine CSIRT sodelujejo s subjekti v javni upravi, gospodarstvu, z raziskovalno-razvojnimi organizacijami, znanstvenimi institucijami, interesnimi združenji in posamezniki.

18. člen
(medsebojni strokovni pregled)

(1) Pristojni nacionalni organ lahko odloči, da z namenom učenja iz skupnih izkušenj, okrepitve medsebojnega zaupanja, doseganja visoke skupne ravni kibernetske varnosti ter okrepitve zmogljivosti in politike na področju kibernetske varnosti, pristopi k medsebojnim strokovnim pregledom, ki jih izvajajo imenovani strokovnjaki s področja kibernetske varnosti drugih držav članic Evropske unije. Evropske komisija in ENISA sodelujeta v medsebojnih strokovnih pregledih kot opazovalki.

(2) Medsebojni strokovni pregled iz prejšnjega odstavka vključuje vsaj eno izmed naslednjih področij:

1. raven izvajanja zahtev glede obvladovanja tveganj za kibernetsko varnost ter obveznosti poročanja iz 20., 21., 25. in 26. člena tega zakona;
2. raven zmogljivosti, vključno z razpoložljivimi finančnimi, tehničnimi in človeškimi viri, ter učinkovitost opravljanja nalog pristojnega nacionalnega organa;
3. operativne zmogljivosti skupin CSIRT;
4. raven izvajanja medsebojne pomoči iz 49. člena tega zakona;
5. raven izvajanja dogovorov o izmenjavi informacij o kibernetski varnosti iz 30. člena tega zakona;
6. posebni čezmejni ali medsektorski vidiki, ki jih opredeli pristojni nacionalni organ.

(3) Za izvajanje medsebojnih strokovnih pregledov iz prvega odstavka se uporablja metodologija, ki jo pripravi Skupina za sodelovanje s pomočjo Evropske komisije in ENISA ter po potrebi mreža skupin CSIRT.

(4) Pristojni nacionalni organ pred začetkom medsebojnega strokovnega pregleda iz prvega odstavka tega člena prek enotne kontaktne točke sodelujočim enotnim kontaktnim točkam drugih držav članic Evropske unije sporoči obseg pregleda, vključno z vidiki, opredeljenimi iz drugega odstavka tega člena.

(5) Pristojni nacionalni organ lahko pred začetkom medsebojnega strokovnega pregleda izvede samooceno vidikov, ki bodo pregledani ob upoštevanju metodologije za samoocenjevanje držav članic Evropske unije, ki jo določi Skupina za sodelovanje ob pomoči Evropske komisije in ENISA. Rezultate samoocene pristojni nacionalni organ posreduje imenovanim strokovnjakom za kibernetsko varnost.

(6) Medsebojni strokovni pregledi obsegajo fizične ali virtualne obiske na kraju samem in izmenjave na daljavo. V primerih iz prvega odstavka tega člena pristojni nacionalni organ brez poseganja v 4. člen tega zakona in v zaščito temeljnih državnih funkcij, kot je nacionalna varnost, ob upoštevanju načela dobrega sodelovanja, imenovanim strokovnjakom za kibernetsko varnost zagotovi informacije, potrebne za njihovo oceno.

(7) Vse informacije, pridobljene v okviru medsebojnega strokovnega pregleda, se uporabljajo izključno v ta namen. Strokovnjaki za kibernetsko varnost, ki sodelujejo pri medsebojnem strokovnem pregledu, občutljivih ali zaupnih informacij, pridobljenih med zadevnim pregledom, ne smejo razkriti tretjim oseba. Kot podlago za delovne metode strokovnjakov za kibernetsko varnost upoštevajo tudi kodekse ravnanja, ki jih pripravi Skupina za sodelovanje ob pomoči Evropske komisije in ENISA.

(8) Pristojni nacionalni organ z namenom sodelovanja pri izvajanju medsebojnih strokovnih pregledov v drugih državah članicah Evropske unije imenuje strokovnjake za kibernetsko varnost na podlagi meril iz metodologije iz tretjega odstavka tega člena. V zvezi z

imenovanimi strokovnjaki za kibernetsko varnost državam članicam Evropske unije, Skupini za sodelovanje, Evropski komisiji in ENISA pred začetkom postopka medsebojnega strokovnega pregleda razkrije vsa tveganja nasprotja interesov v zvezi s strokovnjaki za kibernetsko varnost na način iz četrtega odstavka tega člena.

(9) V primerih iz prvega odstavka tega člena pristojni nacionalni organ lahko nasprotuje imenovanju posameznih strokovnjakov za kibernetsko varnost druge države članice in jo o tem in o razlogih za nasprotovanje obvesti na način iz prejšnjega odstavka.

(10) Strokovnjaki za kibernetsko varnost, ki sodelujejo v medsebojnih strokovnih pregledih, pripravijo poročila o ugotovitvah in sklepih medsebojnih strokovnih pregledov. Poročila vsebujejo priporočila za izboljšanje vidikov, vključenih v medsebojni strokovni pregled. Poročila se predložijo Skupini za sodelovanje in po potrebi mreži skupin CSIRT.

(11) Pristojni nacionalni organ lahko predloži pripombe na osnutek poročila, ki se nanaša na primere iz prvega odstavka tega člena, ki se priložijo poročilu. Pristojni nacionalni organ v primerih iz prvega odstavka tega člena, se lahko odloči, da naredi poročilo javno ali njegovo redigirano različico javno dostopno.

IV. Ukrepi za obvladovanje tveganj in priglasitve incidentov

19. člen
(upravljanje)

(1) Odgovorne osebe pravnih oseb oziroma člani poslovodnih organov (v nadaljnjem besedilu: odgovorne osebe), ki so bistveni ali pomembni subjekti, so odgovorni za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v skladu z določbami tega zakona.

(2) Odgovorne osebe iz prejšnjega odstavka odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih subjekt izvaja zaradi izpolnjevanja obveznosti, določenih s tem zakonom, in nadzirajo njihovo izvajanje.

(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.

(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.

(6) Pristojni nacionalni organ je pristojen za usposabljanje odgovornih oseb iz prvega odstavka tega člena. Program, način in izvajalce izvajanja usposabljanja ter način usposabljanja odgovornih oseb na področju informacijske varnosti, predpiše vlada.

20. člen
(varnostna dokumentacija bistvenih in pomembnih subjektov)

(1) Bistveni in pomembni subjekti za zagotavljanje visoke ravni informacijske in kibernetske varnosti in odpornosti svojih omrežnih in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki temeljita na pristopu upoštevanja vseh nevarnosti in morata obsegati najmanj:

1. natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter določitev njihovih upravljavcev;
2. analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
3. politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti;
4. načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;
5. načrt odzivanja na incidente s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upoštevajo in področne posebnosti bistvenega ali pomembnega subjekta;
7. politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

(2) Bistveni in pomembni subjekti določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, kateri mora obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke ter procese, ki so potrebni za njihovo delovanje ali opravljanje storitev;

(3) Če ima bistveni ali pomembni subjekt za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo dopolni skladno s tem zakonom;

(4) Vlada lahko podrobneje določi vsebino in strukturo varnostne dokumentacije način izvajanja obveznosti iz tega člena. Pri tem vlada upošteva tudi morebitne dokumente ali tehnična priporočila ENISA, Skupine za sodelovanje in dokumente Evropske komisije.

21. člen
(ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov)

(1) Bistveni in pomembni subjekti morajo sprejeti ustrezne, učinkovite in sorazmerne tehnične, operativne in organizacijske ukrepe za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje

tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve (v nadaljevanju: varnostni ukrepi).

(2) Varnostni ukrepi morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščita omrežnih in informacijskih sistemov ter njihovega fizičnega okolja pred incidenti, in morajo obsegati najmanj:

1. podporo vodstva subjekta pri zagotavljanju informacijske in kibernetske varnosti in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;

2. zagotavljanje integritete kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve;

3. osnovne prakse kibernetske higiene in usposabljanje na področju informacijske in kibernetske varnosti;

4. varnost človeških virov, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;

5. izvajanje in upravljanje varnostnih kopij podatkov;

6. zagotavljanje in ohranjanje dnevniških zapisov o delovanju omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, njihovih uporabnikov in administratorjev za obdobje najmanj 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. Ohranjanje dnevniških zapisov se zagotavlja primarno na ozemlju Republike Slovenije, sekundarno pa se lahko zagotavlja na ozemlju Evropske unije, razen subjektov s področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, kateri lahko ohranjanje dnevniških zapisov v celoti zagotavlja na ozemlju Evropske unije;

7. upravljanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z določitvijo ustrezne odgovornosti za njihovo zaščito;

8. politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;

9. upravljanje prometa in komunikacij;

10. varnost dobavne verige z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za ključne dobavitelje ali ponudnike storitev, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;

11. fizično in tehnično varovanje prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev;

12. varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter obravnavanjem in razkrivanjem ranljivosti;

13. upravljanje in preprečevanje izrab tehničnih ranljivosti;

14. zaščita pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov;

15. uporabo večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost in

16. uporabo varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je glede na dejavnost subjekta to primerno.

(3) Varnostni ukrepi iz prejšnjega odstavka morajo ob upoštevanju najsodobnejših in ustreznih evropskih in mednarodnih standardov ter stroškov izvajanja zagotavljati raven varnosti omrežnih in informacijskih sistemov, ki ustreza obstoječim oziroma prepoznanim tveganjem. Pri ocenjevanju sorazmernosti varnostnih ukrepov bistveni in pomembni subjekti ustrezno upoštevajo:

- stopnjo izpostavljenosti tveganjem,

- velikost subjekta,

- verjetnost pojava incidentov in

- resnost morebitnih incidentov, vključno z njihovim družbenim in gospodarskim vplivom.

(4) Dnevniški zapisi morajo biti hranjeni na način, ki zagotavlja njihovo celovitost, avtentičnost, razpoložljivost in zaupnost v primeru incidentov.

(5) Bistveni in pomembni subjekti morajo pri oceni in izvedbi ustreznih varnostnih ukrepov za varnost dobavne verige 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 kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige ter lahko preverjajo njihovo izvajanje pri dobaviteljih in ponudnikih storitev. 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) Bistveni ali pomembni subjekti najmanj enkrat letno oziroma v rednih časovnih obdobjih, ki jih opredelijo v politiki in postopkih za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost in ob zaznanih ranljivostih, preverjati izpolnjevanje varnostnih ukrepov iz tretjega odstavka tega člena. V primeru ugotovljenega pomanjkljivega ali neustreznega izvajanja varnostnih ukrepov morajo brez nepotrebnega odlašanja sprejeti vse potrebne, ustrezne in sorazmerne popravne ukrepe.

(7) 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 zaupanja pri sprejemu varnostnih ukrepov iz tretjega odstavka tega člena upoštevajo izvedbene akte Evropske komisije iz prvega pododstavka petega odstavka 21. člena

Direktive (EU) 2022/2555, s katerimi ta določi tehnične in metodološke zahteve za varnostne ukrepe.

(8) Bistveni in pomembni subjekti, ki niso navedeni v prejšnjem odstavku, pri sprejemu varnostnih ukrepov iz tretjega odstavka tega člena, upoštevajo morebitne izvedbene akte Evropske komisije, s katerimi ta določi tehnične, metodološke ter sektorske zahteve za varnostne ukrepe.

(9) Bistveni in pomembni subjekti ne smejo uporabljati informacijsko-komunikacijskih rešitev, ki imajo aktivno izkoriščane ranljivosti brez dodatne izvedbe ocene tveganja in uvedenih ustreznih dodatnih varnostnih ukrepov, ki znižajo stopnjo tveganja na sprejemljivo raven.

(10) Če bistveni ali pomembni subjekti za opravljanje svoje dejavnosti črpajo vhodne podatke in informacije iz ključnih delov nacionalnovarnostnega sistema, vzpostavijo vse potrebne varnostne zahteve ob soglasju pristojnega ministrstva ali vladne službe za posamezni ključni del nacionalnovarnostnega sistema.

(11) 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 zadevnih dokumentih Evropske komisije. Pri tem vlada upošteva tudi morebitne dokumente ali tehnična priporočila ENISA ter Skupine za sodelovanje.

(12) Upravljavec centralnega informacijsko-komunikacijskega sistema mora določiti minimalne varnostne zahteve informacijske varnosti povezanim subjektom ter zagotoviti, da jih povezani subjekti izpolnjujejo. Za namen pravočasnega odzivanja na kibernetske grožnje in preprečevanja škodljivih posledic morebitnega težjega ali kritičnega incidenta ter zaradi izvajanja kibernetske obrambe je upravljavec centralnega informacijsko-komunikacijskega sistema pooblaščen, da izvede ustrezne, nujne in sorazmerne ukrepe za zaščito centralnega informacijsko-komunikacijskem sistema. Ukrepi vključujejo tudi začasni odklop posameznega povezanega subjekta iz centralnega informacijsko-komunikacijskega sistema dokler ugotovljena tveganja niso odpravljena.

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.

23. člen
(certificiranje)

(1) Certificiranje za kibernetsko varnost pomeni potrditev, da so bili proizvodi IKT, storitve IKT in postopki IKT ocenjeni v skladu z veljavnimi evropskimi certifikacijskimi shemami za kibernetsko varnost iz izvedbenih aktov Evropske komisije sprejetimi na podlagi člena 49 Uredbe (EU) 2019/881 (v nadaljnjem besedilu evropske certifikacijske sheme za kibernetsko varnost) in da izpolnjujejo v teh shemah določene varnostne zahteve.

(2) Certificiranje za kibernetsko varnost se izvaja v skladu z Uredbo (EU) 2019/881 in evropskimi certifikacijskimi shemami za kibernetsko varnost.

(3) Pristojni nacionalni organ izvaja naloge nacionalnega certifikacijskega organa za kibernetsko varnost iz 22. točke drugega odstavka 9. člena tega zakona v skladu z Uredbo (EU) 2019/881 in evropskimi certifikacijskimi shemami za kibernetsko varnost.

(4) Javni zavod Slovenska akreditacija izvaja naloge nacionalnega akreditacijskega organa iz Uredbe (EU) 2019/881 in akreditira organe za ugotavljanje skladnosti, ki izpolnjujejo pogoje iz prej navedene uredbe.

(5) Organ za ugotavljanje skladnosti za potrebe tega zakona je organ za ugotavljanje skladnosti iz zakona, ki ureja tehnične zahteve za proizvode in ugotavljanje skladnosti, ki izpolnjuje dodatne zahteve iz priloge Uredbe (EU) 2019/881.

(6) Organi za ugotavljanje skladnosti na podlagi Uredbe (EU) 2019/881 izdajo evropski certifikat kibernetske varnosti, ki se nanaša na osnovno ali znatno raven zanesljivosti, na podlagi meril, vključenih v evropsko certifikacijsko shemo za kibernetsko varnost razen, če evropska certifikacijska shema za kibernetsko varnost določa, da mora evropske certifikate kibernetske varnosti, ki izhajajo iz te sheme, izdati le javni organ, ki je akreditiran kot organ za ugotavljanje skladnosti.

(7) Kadar evropska certifikacijska shema za kibernetsko varnost zahteva visoko raven zanesljivosti, lahko evropski certifikat kibernetske varnosti na podlagi te sheme izda nacionalni certifikacijski organ za kibernetsko varnost oziroma organ za ugotavljanje skladnosti, na katerega je pristojni nacionalni organ prenesel pooblastilo izdajanja evropskih certifikatov kibernetske varnosti.

(8) Nacionalni certifikacijski organ za kibernetsko varnost z odločbo lahko odvzame evropski certifikat kibernetsko varnost, ki ga izda pristojni organ iz šestega ali prejšnjega odstavka tega člena, kadar tak certifikati ni v skladu z Uredbo (EU) 2019/881 ali z evropskimi certifikacijskimi shemami za kibernetsko varnost sprejetimi na podlagi člena 49 Uredbe (EU) 2019/881.

(9) Evropski certifikat kibernetske varnosti pomeni dokument, ki ga izda organ iz šestega odstavka tega člena ali iz prejšnjega odstavka in potrjuje, da je bil zadevni proizvod IKT, storitev IKT ali postopek IKT ocenjen glede skladnosti s posebnimi varnostnimi zahtevami, določenimi v evropski certifikacijski shemi za kibernetsko varnost. Izjava EU o skladnosti ima pomen kot ga določa zakon ki ureja pogoje dajanja proizvodov na trg, dostopnosti na trgu in varne uporabe, tehnične zahteve za proizvode, postopke ugotavljanja skladnosti, zahteve in postopek določitve organov, ki sodelujejo v postopkih ugotavljanja skladnosti tehnične zahteve za proizvode in o ugotavljanju skladnosti.

(10) Fizične ali pravne osebe imajo pravico, da vložijo pritožbo pri izdajatelju evropskega certifikata kibernetske varnosti. Kadar se pritožba nanaša na evropski certifikat kibernetske varnosti, ki ga je izdal organ za ugotavljanje skladnosti v skladu s sedmim odstavkom tega člena, se pritožba vloži pri nacionalnem certifikacijskem organu za kibernetsko varnost. Fizične in pravne osebe imajo tudi pravico, da vložijo pritožbo glede izjav EU o skladnosti pri nacionalnem certifikacijskem organu za kibernetsko varnost.

(11) Organ, pri katerem je bila vložena pritožba preizkusi vsebino pritožbe in obvesti pritožnika o napredku postopka ali o odstopu pritožbe v reševanje nacionalnemu

certifikacijskemu organu za kibernetsko varnost, ki odloči o pritožbi. Ob vročitvi odločbe nacionalni certifikacijski organ za kibernetsko varnost pritožnika obvesti o pravici do vložitve tožbe v upravnem sporu zoper izdano odločbo, ki se vloži na sedežu Upravnega sodišča Republike Slovenije.

(12) Kadar na podlagi sedmega ali osmega odstavka tega člena odloča nacionalni certifikacijski organ za kibernetsko varnost, je zoper njegovo odločbo dovoljena le tožba v upravnem sporu, ki se vloži v skladu s prejšnjim odstavkom tega člena.

(13) Sodno varstvo iz devetega odstavka tega člena in prejšnjega odstavka vključuje tudi nepravilno izdajo, opustitev izdaje ali priznanje evropskega certifikata kibernetske varnosti, ki ga je izdal za to pristojni organ druge države članice Evropske unije in ga imajo v lasti zadevne fizične ali pravne osebe. Nanaša se tudi na opustitev ukrepanja oziroma molk pritožbenega organa iz prejšnjega odstavka glede pritožbe, ki je bila pri njem vložena.

(14) Bistveni in pomembni subjekti iz kategorij, ki jih določi Evropska komisija z delegiranim aktom, morajo za obvladovanje tveganj za kibernetsko varnost uporabljati v njem določene certificirane proizvode IKT, storitve IKT in procese IKT ali pridobiti certifikat na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49 Uredbe (EU) 2019/881.

(15) Bistveni in pomembne subjekti pri izvajanju ukrepov iz 21. člena tega zakona, prednostno uporabljajo kvalificirane storitve zaupanja in tiste proizvode IKT, storitve IKT ali postopke IKT, kjer je proizvajalec ali ponudnik izdal in podpisal izjavo Evropske unije o skladnosti proizvoda IKT, storitve IKT ali postopka IKT oziroma je ugotavljanje skladnosti proizvoda IKT, storitve IKT ali postopka IKT z zahtevami evropskih certifikacijskih shem za kibernetsko varnost izvedel kateri izmed organov za ugotavljanje skladnosti držav članic EU.
(16) Ne glede na prejšnji odstavke vlada lahko zaradi potrebe po višji ravni kibernetske varnosti iz razlogov zagotavljanja nacionalne varnosti, določenim kategorijam bistvenih subjektov predpiše obvezno uporabo, v okviru evropske certifikacijske sheme za kibernetsko varnost, certificiranih proizvodov IKT, storitev IKT ali postopkov IKT. Pri tem lahko predpiše tudi določeno raven njihove zanesljivosti oziroma varnosti, ki jo zagotavljajo.

24. člen
(standardizacija)

(1) Bistveni in pomembni subjekti zaradi zagotovitve skladnega izvajanja ukrepov iz 20. in 21. 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.

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 in nacionalnim načrtom odzivanja iz drugega odstavka 11. člena tega zakona priglasijo vse incidente, ki imajo pomemben vpliv

na zagotavljanje njihovih storitev. Pri tem se incident šteje za pomembnega (v nadaljnjem besedilu pomemben incident), 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) Pri vrednotenju pomembnosti incidenta bistveni in pomembni subjekti upoštevajo prizadetost omrežnih in informacijskih sistemov, zlasti njihov pomen pri zagotavljanju storitev subjekta, resnost in tehnične značilnosti kibernetske grožnje in njihovega vpliva na uporabnike, obstoječe ranljivosti, ki se izkoriščajo, ter izkušnje subjekta s podobnimi incidenti. Bistveni in pomembni subjekti pri priglašanju iz prejšnjega odstavka upoštevajo morebitne izvedbene akte Evropske komisije iz prvega pododstavka enajstega odstavka 23. člena Direktive (EU) 2022/2555, s katerimi ta podrobneje določi vrsto informacij, obliko in postopek priglasitve ter prostovoljne priglasitve in obvestila.

(3) 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, kot tudi ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, pri priglašanju iz prejšnjega odstavka, upoštevajo izvedbene akte Evropske komisije iz drugega pododstavka enajstega odstavka 23. člena Direktive (EU) 2022/2555, v katerih so zanje podrobneje določeni primeri, ko se incident šteje za pomembnega.

(4) Bistveni in pomembni subjekti iz prvega odstavka tega člena, ki niso subjekti iz prejšnjega odstavka upoštevajo morebitne izvedbene akte Evropske komisije iz drugega pododstavka enajstega odstavka 23. člena Direktive (EU) 2022/2555, v katerih so zanje podrobneje določeni primeri, ko se incident šteje za pomembnega. Če Evropska komisija takšnih izvedbenih aktov ne sprejme, se za te subjekte upošteva metodologija za določitev pomembnosti incidenta, kot je opredeljena v nacionalnem načrtu odzivanja.

(5) Bistveni in pomembni subjekti pristojni skupini CSIRT sporočijo vse potrebne informacije, da le-ta določi čezmejni vpliv pomembnega incidenta. V primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta se ustrezna informacija pravočasno posreduje enotni kontaktni točki v skladu s 26. členom tega zakona.

(6) Kadar je ustrezno bistveni in pomembni subjekti uporabnike svojih storitev brez nepotrebnega odlašanja uradno obvestijo o pomembnih incidentih iz prvega odstavka tega člena, ki bodo verjetno negativno vplivali na zagotavljanje teh storitev.

(7) Bistveni in pomembni subjekti brez nepotrebnega odlašanja uporabnikom svojih storitev, ki bi jih pomembna kibernetska grožnja lahko prizadela, sporočijo vse ukrepe ali sredstva, ki jih lahko ti uporabniki sprejmejo v odziv na to grožnjo. Kadar je ustrezno, subjekti zadevne uporabnike obvestijo tudi o sami pomembni kibernetski grožnji.

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 pomembnega 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;
- 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 pomembnega 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.

(3) Pristojna skupina CSIRT brez nepotrebnega odlašanja in po možnosti v 24 urah po prejemu zgodnjega opozorila iz 1. točke prvega odstavka tega člena, odgovori priglasitvenemu subjektu, vključno z začetnimi povratnimi informacijami o pomembnem incidentu in, na zahtevo priglasitvenega subjekta, z usmeritvami ali operativnim nasvetom glede izvajanja morebitnih blažilnih ukrepov. Pristojna skupina CSIRT brez nepotrebnega odlašanja o priglasitvi seznani pristojni nacionalni organ ter ga obvešča o opravljenih aktivnostih. Skupina CSIRT na zahtevo zadevnega subjekta zagotovi dodatno tehnično podporo. Kadar obstajajo razlogi za sum, da ima incident znake kaznivega dejanja, skupina CSIRT zagotovi tudi usmeritve o poročanju o pomembnih incidentih organom kazenskega pregona.

(4) V primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta pristojna skupina CSIRT nemudoma zagotovi pristojnemu nacionalnemu organu priglašene informacije o incidentu iz prvega odstavka tega člena. Kadar pristojni nacionalni organ ali skupina CSIRT menita, da je to potrebno, zlasti kadar pomemben incident zadeva dve ali več držav članic, enotna kontaktna točka na zahtevo, brez nepotrebnega odlašanja, o pomembnem incidentu obvesti enotne kontaktne točke drugih prizadetih držav članic in ENISA. To obvestilo vključuje vrsto informacij, prejetih v skladu s prvim odstavkom tega člena. Pri tem enotna kontaktna točka v skladu s pravom Evropske unije ali pravom Republike Slovenije zaščiti varnost in poslovne interese zavezanca ter zaupnost predloženih informacij, ki jih slednji zagotovi v svoji priglasitvi.

(5) Enotna kontaktna točka vsake tri mesece predloži zbirno poročilo na ENISA, vključno z anonimizirani in zbirnimi podatki o incidentih, pomembnih kibernetskih grožnjah in skorajšnjih incidentih, priglašenih v skladu s prvim odstavkom tega člena in 31. členom tega zakona.

(6) Kadar je ozaveščenost javnosti potrebna za preprečitev pomembnega incidenta ali obravnavo pomembnega incidenta, ki je v teku, ali kadar je razkritje pomembnega incidenta kako drugače v javnem interesu, pristojni nacionalni organ po posvetovanju z zadevnim zavezancem obvesti javnost o pomembnem incidentu ali zahteva, da to stori zavezanec.

(7) Kadar je pristojni nacionalni organ prek enotne kontaktne točke obveščen o pomembnem čezmejnem ali medsektorsko pomembnem incidentu, ki ima vpliv tudi v Republiki Sloveniji, lahko po posvetovanju s subjektom, ki je priglasil incident, obvesti javnost o pomembnem incidentu ali zahteva, da to stori zavezanec tudi, kadar je bil incident priglašen v drugi državi članici Evropske unije.

(8) Pristojni nacionalni organ zagotovi pristojnemu nacionalnemu organu iz zakona, ki ureja kritično infrastrukturo, informacije o pomembnih incidentih, incidentih, kibernetskih grožnjah in skorajšnjih incidentih, ki so jih v skladu prvim odstavkom 25. člena tega zakona ali pri prostovoljni priglasitvi iz člena 31. člena tega zakona priglasili bistveni subjekti, ki so identificirani kot kritični subjekti na podlagi predpisov, ki urejajo kritično infrastrukturo.

(9) Pristojna skupina CSIRT o pomembnem incidentu nemudoma obvesti pristojni nacionalni organ, ki vodi seznam pomembnih incidentov. Pristojni nacionalni organ o incidentu, ki bi lahko imel večji medsektorski vpliv oziroma bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti Republike Slovenije, obvesti Nacionalni center za krizno upravljanje, lahko pa obvesti tudi druge pristojne organe, s katerimi sodeluje na nacionalni ravni v skladu s 17. členom tega zakona.

(10) Priglasitve pomembnih incidentov in medsebojno sodelovanje iz tega člena se izvaja tudi po namenski digitalni platformi, ki jo vzpostavijo skupine CSIRT in pristojni nacionalni organ. Do vzpostavitve navedene platforme se zagotovi varnost prenesenih podatkov po elektronski poti.

(11) Pristojni nacionalni organ za namen izvajanja nalog iz tega zakona vodi tudi:

- skupen seznam pomembnih incidentov, ki vsebuje podatke iz končnih poročil o incidentih iz tega člena in
- seznam omrežnih in informacijskih sistemov, delov omrežja in digitalnih oziroma elektronskih komunikacijskih storitev zavezancev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti, ki je varovani podatek pristojnega nacionalnega organa.

V. Pristojnost in registracija

27. člen
(pristojnost in teritorialnost)

(1) Pristojni nacionalni organ in pristojne skupine CSIRT so pristojne za zavezance iz tretjega člen tega zakona, ki jih je ustanovila Republika Slovenija ali imajo sedež v Republiki Sloveniji, razen za:

- ponudnike javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev, ki spadajo v pristojnost države članice Evropske unije, v kateri zagotavljajo svoje storitve;
- 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 iskalnikov in platform za storitve družbenega mreženja, ki spadajo v pristojnost države članice, v kateri imajo glavni sedež v Evropski uniji v skladu z drugim odstavkom tega člena.

(2) Za namene tega zakon se za subjekte iz druge alineje prejšnjega odstavka šteje, da imajo glavni sedež v Evropski uniji v državi članici Evropske unije, kjer se sprejme večina odločitev v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. Če te države članice Evropske unije ni mogoče določiti ali če se te odločitve ne sprejemajo v Evropski uniji, se šteje, da je glavni sedež v državi članici Evropske unije, kjer se izvajajo operacije v zvezi s kibernetsko varnostjo. Če te države članice Evropske unije ni mogoče določiti, se šteje, da je glavni sedež v državi članici, kjer ima zadevni subjekt sedež z največjim številom zaposlenih v Evropski uniji.

(3) Če subjekt iz druge alineje prvega odstavka tega člena, ki nima sedeža v Evropski uniji, v njej pa zagotavlja takšne storitve, določi sedež svojega predstavnika za Evropsko unijo v Republiki Sloveniji, kjer tudi zagotavlja takšne storitve, spada v pristojnost pristojnega nacionalnega organa in pristojne skupine CSIRT. Predstavnik zastopa subjekt v zvezi z obveznostmi na podlagi tega zakona.

(4) Če subjekt iz druge alineje prvega odstavka tega člena ni imenoval predstavnika v Evropski uniji opravlja pa storitve v Republiki Slovenije, lahko pristojni nacionalni organ predlaga uvedbo sodnih postopkov proti subjektu zaradi kršitve tega zakona. Imenovanje predstavnika s strani subjekta ne posega v sodne postopke, ki se lahko uvedejo proti samemu subjektu.

(5) Če pristojni nacionalni organ prejme zahtevek za medsebojno pomoč na podlagi 49. člena tega zakona v zvezi s subjektom iz druge alineje prvega odstavka tega člena, lahko v mejah zahtevka inšpektor za informacijsko varnost sprejme ustrezne nadzorne in izvršilne ukrepe v zvezi z zadevnim subjektom, ki opravlja storitve ali ima omrežni in informacijski sistem na ozemlju Republike Slovenije.

28. člen
(zbiranje informacij za register ponudnikov storitev pri ENISA)

(1) Subjekti, ki sodijo v pristojnost pristojnega nacionalnega organa v skladu s prvim odstavkom 27. člena tega zakona in so ponudniki storitev DNS, registrov TLD imen, registracije domenskih imen ali so ponudniki storitev računalništva v oblaku, storitev podatkovnih centrov, omrežij za dostavo vsebine, upravljanih storitev, upravljanih varnostnih storitev, kot tudi spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, pristojnemu nacionalnemu organu zaradi namena olajšanega sodelovanja zavezanih ponudnikov teh storitev s pristojnimi organi pri obvladovanju skorajšnjega incidenta, incidenta ali pomembnega incidenta podajo naslednje informacije:

1. ime subjekta;
2. ustrezni sektor, podsektor in vrsto subjekta iz Priloge I ali II, kadar je to ustrezno;
3. naslov njegovega glavnega sedeža in njegovih drugih zakonitih sedežev v Evropski uniji ali, če nima sedeža v Evropski uniji, njegovega predstavnika, imenovanega v skladu s tretjim odstavkom 27. člena tega zakona;
4. posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjekta in po potrebi njegovega zastopnika, imenovanega v skladu s tretjim odstavkom 27. člena tega zakona;
5. države članice, v katerih subjekt opravlja storitve, ter
6. bloke subjektu dodeljenih številk avtonomnih sistemov in javnih naslovov IP.

(2) Subjekti iz prejšnjega odstavka pristojni nacionalni organ obvestijo o vsaki spremembi informacij, ki so jih predložili v skladu s prejšnjim odstavkom. Obvestilo o spremembi subjekti predložijo nemudoma oziroma v vsakem primeru v treh mesecih od datuma spremembe informacij.

(3) Subjekti iz prvega odstavka predložijo informacije iz prvega in drugega odstavka tega člena pristojnemu nacionalnemu organu prek mehanizma za samoregistracijo zavezancev iz prvega odstavka 7. člena tega zakona. Do vzpostavitve samoregistracijskega mehanizma se informacije posredujejo v digitalni obliki na elektronski naslov pristojnega nacionalnega organa.

(4) Pristojni nacionalni organ v vlogi enotne kontaktne točke po prejemu informacij iz prvega in drugega odstavka, razen informacij iz 6. točke prvega odstavka tega člena, te informacije brez nepotrebnega odlašanja predloži ENISA za potrebe njene vzpostavitve in vzdrževanja registra ponudnikov storitev iz prvega odstavka tega člena.

29. člen
(podatkovna zbirka o registraciji domenskih imen)

(1) Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen zaradi zagotovitve varnosti, stabilnosti in odpornosti DNS z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v posebni podatkovni zbirki, pri čemer za zbrane osebne podatke upoštevajo predpise s področja varstva osebnih podatkov.

(2) Podatkovna zbirka iz prejšnjega odstavka mora vsebovati potrebne informacije o registraciji domenskih imen, ki vsebujejo potrebne informacije za identifikacijo imetnikov domenskih imen in kontaktnih točk, ki upravljajo domenska imena v okviru vrhnjih domenskih imen, in navezavo stika z njimi. Take informacije vključujejo:

- domensko ime;
- datum registracije;
- ime imetnika domenskega imena , njegov kontaktni elektronski naslov in telefonsko številko;
- kontaktni elektronski naslov in telefonsko številko kontaktne točke, ki upravlja domensko ime, če se razlikuje od naslova imetnika domenskega imena.

(3) Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, vzpostavijo politike in postopke, vključno s postopki preverjanja, ki zagotavljajo, da podatkovne zbirke iz prvega odstavka tega člena vključujejo točne in popolne informacije, pri čemer se upošteva, da se mora preveriti po vsaj en kontaktni podatek iz tretje in četrte alineje prejšnjega odstavka. Te politike in postopki morajo biti javno dostopni.

(4) Subjekti iz prvega odstavka tega člena po registraciji domenskega imena brez nepotrebnega odlašanja podatke o registraciji, ki niso osebni podatki, naredijo javno dostopne.

(5) Subjekti iz prvega odstavka tega člena omogočijo dostop do podatkov o registraciji posameznih domenskih imen na podlagi zakonitih in ustrezno utemeljenih zahtevkov oseb, ki imajo upravičen razlog za dostop, v skladu s predpisom s področja varstva osebnih podatkov. Subjekti iz prvega odstavka tega člena odgovorijo brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah od prejema kakršnih koli zahtevkov za dostop. Politike in postopki v zvezi z razkritjem teh podatkov morajo biti javno dostopni.

(6) Izpolnjevanje obveznosti od prvega do petega odstavka tega člena ne sme povzročiti podvajanja zbiranja podatkov o registraciji domenskih imen. V ta namen morajo registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen medsebojno sodelovati.

VI. Izmenjava informacij

30. člen
(dogovori o izmenjavi informacij o kibernetski varnosti)

(1) Zavezanci na podlagi tega zakona ter, kadar je to ustrezno, tudi drugi subjekti, si lahko prostovoljno izmenjujejo ustrezne informacije o kibernetski varnosti, vključno z informacijami, ki se nanašajo na kibernetske grožnje, skorajšnje incidente, ranljivosti, tehnike in postopke, kazalnike ogroženosti, sovražne taktike, specifične informacije o grožnji in akterju, opozorila glede kibernetske varnosti in priporočila glede konfiguracije orodij za kibernetsko varnost za zaznavo zlonamernih kibernetskih aktivnosti, kadar taka izmenjava informacij:

- pripomore k preprečevanju in odkrivanju incidentov, odzivanju nanje ali okrevanju po njih ali k ublažitvi njihovega vpliva;
- zvišuje raven kibernetske varnosti, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem ranljivosti, tehnikami odkrivanja, omejevanja in preprečevanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja ali spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

(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.

(3) Pristojni nacionalni organ spodbuja sklenitev dogovorov o izmenjavi informacij o kibernetski varnosti iz prejšnjega odstavka, ki lahko vključujejo operativne elemente, vključno glede uporabe namenskih digitalnih platform in orodij za avtomatizacijo ter vsebine in pogoje za dogovore o izmenjavi informacij.

(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.

(5) Na zaprosilo zavezancev iz tega zakona pristojni nacionalni organ ali skupini CSIRT lahko sodelujejo pri posamičnem dogovoru iz prejšnjega odstavka in pri tem določijo pogoje glede informaciji, ki jih dajo na voljo.

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.

(3) Prostovoljna priglasitev iz prvega in prejšnjega odstavka skupine CSIRT obravnavajo v skladu s postopkom iz 26. člena tega zakona. Pri prostovoljnem poročanju za priglasitveni subjekt ne veljajo nikakršne dodatne obveznosti, kar pa ne vpliva na preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

(4) Pristojni skupini CSIRT po potrebi informacije o priglasitvah, prejetih v skladu s tem členom, kadar je potrebno, posredujejo pristojnemu nacionalnemu organu v vlogi enotne kontaktne točke, pri čemer poskrbijo za zaupnost in ustrezno varstvo informacij, ki jih je posredoval priglasitveni subjekt.

(5) Pristojni skupini CSIRT pred prostovoljnimi priglasitvami lahko prednostno obravnavata obvezne priglasitve. Pri določanju vrstnega reda obdelave prostovoljnih priglasitev upoštevata vpliv prostovoljno priglašenih incidentov na neprekinjeno izvajanje storitev zavezanih subjektov ter morebitni čezmejni vpliv.

(6) Prostovoljne priglasitve, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje storitev zavezanih subjektov in imajo zanemarljiv čezmejni vpliv, se obdela le, kadar takšna obdelava skupinama CSIRT ne pomeni nesorazmernega ali neupravičenega bremena.

(7) Prostovoljna priglasitev ustreznih informacij iz tega člena se lahko izvaja tudi po namenski digitalni platformi iz desetega odstavka 26. člena tega zakona.

VII. Vrednotenje incidenta, ocena ogroženosti in ukrepanje

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 organa državne uprave. 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 varnostni dogodek - zaznane kibernetske aktivnosti, ki nimajo vpliva na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. Zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci;
- C5 skorajšnji incident - pomeni varnostni dogodek, ki bi lahko ogrozil razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni, vendar se je preprečilo, da bi se ta dogodek uresničil, ali se ni uresničil;

- C4 lažji incident - enkraten incident, ki glede na parametre določitve pomembnosti vpliva incidenta zadevnemu subjektu ni povzročil in ne more povzročiti znatne operativne motnje pri opravljanju storitev ali finančne izgube ter ni vplival in ne more vplivati na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode. Kadar takšen incident nima negativnega medsektorskega vpliva ali negativnega vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja;
- C3 težji incident - enkraten pomemben incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju, ki je glede na parametre določitve pomembnosti vpliva incidenta 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 ali ima negativen medsektorski vpliva ali negativen vpliv na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja;
- C2 težji incident - enkraten pomemben incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju, kadar obstaja možnost, da preraste v kritični incident;
- C1 kritični incident - pomemben incident, ki poleg že opredeljenih vplivov, povzroči tudi oteženo delovanje države, še posebej izvajanje nalog obrambe, notranje varnosti ter zaščite in reševanja, oziroma delno onemogoči delovanje vsaj treh visoko kritičnih sektorjev ali enega v celoti.

(2) Pristojni nacionalni organ na podlagi podatkov in stopnje incidenta iz prejšnjega odstavka, ki mu jih sproti posredujejo skupine CSIRT, oceni ali gre hkrati tudi za kibernetski incident velikih razsežnosti ali krizo.

(3) Pristojni nacionalni organ mora o kritičnem incidentu nemudoma obvestiti vlado in SNAV, lahko pa ju glede na presojo relevantnih okoliščin obvesti tudi o težjem incidentu kadar obstaja možnost, da preraste v kritični incident.

(4) Pristojni nacionalni organ lahko zavezancu v primeru težjega incidenta C3, C2 ali kritičnega incidenta C1 s pisno odločbo, v nujnih primerih pa tudi ustno, določi takšne primerne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic.

(5) V primeru ko pristojni nacionalni organ oceni da nima vseh dejstev nujno potrebnih za opredelitev težjega incidenta ali kritičnega incidenta ter preprečitev nadaljnjih škodljivih posledic incidenta, lahko s pisno odločbo, v nujnih primerih pa tudi ustno od zavezanca, zahteva posredovanje dodatnih podatkov in pojasnil ter določi rok za njihovo posredovanje.

(6) Ukrepi, izdani na podlagi četrtega odstavka tega člena, se določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz četrtega odstavka tega člena. Zoper odločbo iz četrtega in prejšnjega odstavka tega člena ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.

(7) Direktor pristojnega nacionalnega organa lahko z namenom preprečitve nastanka krize ali njenega obvladovanja ali zaradi hitrejšega obvladovanja razmer in omejevanja nadaljnjih škodljivih posledic težjega incidenta C2 ali kritičnega incidenta C1 izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih. Odredba se izda pisno, izjemoma, če razmere

to onemogočajo, se izda ustno in naknadno tudi pisno, takoj ko je to mogoče. V odredbi se določita zlasti vrsta in obseg del, ki jih je treba opraviti ter rok.

(8) Pristojni nacionalni organ o ukrepih iz četrtega in sedmega odstavka tega člena obvesti vlado in SNAV.

33. člen
(ocena ogroženosti)

(1) Pristojni nacionalni organ na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, s katerimi razpolaga ali jih pridobi, izdela oceno ogroženosti kibernetske varnosti v Republiki Sloveniji (v nadaljnjem besedilu: ogroženost), pri čemer ogroženost vrednoti kot:

- zelo nizka ogroženost;
- nizka ogroženost;
- srednja ogroženost;
- visoka ogroženost;
- kritična ogroženost.

(2) Ne glede na oceno ogroženosti iz prejšnjega odstavka zavezanci izvajajo najmanj ukrepe iz 20. in 21. člena tega zakona.

(3) V primeru, da je ocena ogroženosti ovrednotena kot srednja, pristojni nacionalni organ o tem obvesti zavezance, pri tem jim lahko priporoči izvedbo dodatnih ukrepov za varnost omrežij ali informacijskih sistemov. Pristojni nacionalni organ lahko o tem obvesti tudi splošno javnost prek svojih spletnih strani in sredstev javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe.

(4) Pristojni nacionalni organ v primerih, da je ocena ogroženosti ovrednotena kot kritična o tem nemudoma obvesti vlado in SNAV, lahko pa ju, glede na presojo relevantnih okoliščin in informacij, obvesti tudi v primeru, da je ogroženost ovrednotena kot visoka. O oceni ogroženosti visoka ali kritična, pristojni nacionalni organ obvesti zavezance, lahko pa obvesti tudi splošno javnost prek svojih spletnih strani in sredstev javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe. Pristojni nacionalni organ o preklicu ali spremembi ocene ogroženosti kritično, lahko pa tudi visoko obvesti predhodno obveščene deležnike iz tega odstavka.

(5) V primerih ocene ogroženosti visoka morajo zavezanci nemudoma pričeti izvajati vsaj naslednje dodatne varnostne ukrepe, ki jih izvajajo do preklica takšne ogroženosti:

- spremljanje varnostnih obvestil pristojne skupine CSIRT oziroma pristojnega nacionalnega organa, ki se nanašajo na razglašeno ogroženost visoka;
- preverba ustreznega ohranjanja dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja;
- takojšnje izvajanje morebitnih varnostnih navodil skupine CSIRT oziroma pristojnega nacionalnega organa, ki se nanašajo na razglašeno ogroženost visoka;
- poročanje o stanju varnosti njihovih omrežij in informacijskih sistemov in o izvajanju morebitnih ukrepov na način kot to izhaja iz morebitnega varnostnega navodila iz prejšnje alineje.

(6) V primerih ocene ogroženosti kritična morajo zavezanci poleg ukrepov iz prejšnjega odstavka nemudoma pričeti izvajati tudi naslednje dodatne varnostne ukrepe, ki jih izvajajo do preklica takšne ogroženosti:

- stalno spremljanje varnostnih obvestil pristojne skupine CSIRT oziroma pristojnega nacionalnega organa, ki se nanašajo na razglašeno ogroženost kritična;
- preverba ustreznega delovanja beleženja in ohranjanja dnevniških zapisov iz 6. točke drugega odstavka 21. člena tega zakona ter poročanje o tem in morebiti izvedenih aktivnostih v skladu s šesto alinejo tega odstavka;
- spremljanje celotnega prometa na svojem omrežju z namenom ugotavljanja anomalij in poročanje o tem ter morebitnih izvedenih aktivnostih v skladu s šesto alinejo tega odstavka;
- takojšnje izvajanje morebitnih varnostnih navodil skupine CSIRT oziroma pristojnega nacionalnega organa, ki se nanašajo na razglašeno ogroženost kritična;
- takojšnja priglasitev morebitnih incidentov ne glede na roke iz 25. člena tega zakona;
- vsaj tedensko poročanje o stanju varnosti njihovih omrežij in informacijskih sistemov kot tudi glede zaznav varnostnih dogodkov in njihovih s tem povezanih aktivnosti kot tudi o izvajanju morebitnih varnostnih navodil iz druge alineje tega odstavka pristojni skupini CSIRT;
- pogostejše poročanje vsebin iz prejšnje alineje pristojni skupini CSIRT, če tako izhaja iz varnostnega navodila iz druge alineje tega odstavka.

(7) Ne glede na peti in prejšnji odstavek tega člena lahko pristojni nacionalni organ zavezancu s pisno odločbo, v nujnih primerih pa tudi ustno, določi primerne in sorazmerne ukrepe, kot je potrebno za zmanjšanje ogroženosti. Zavezancu se pisni odpravek ustne odločbe vroči čim prej, vendar najkasneje v roku 48 ur po ustni odločbi.

(8) Ukrepi, izdani na podlagi prejšnjega odstavka, se določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz prejšnjega odstavka. Zoper odločbo iz prejšnjega odstavka ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.

(9) Direktor pristojnega nacionalnega organa lahko z namenom nižanja ocene ogroženosti visoka ali kritična ter posledično zaradi preprečitve nastanka krize ali njenega obvladovanja izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih, varnostno operativnih centrih organov državne uprave oziroma skupinah CSIRT. Odredba se izda pisno, izjemoma, če razmere to onemogočajo, se izda ustno in naknadno tudi pisno, takoj ko je to mogoče. V odredbi se določita zlasti vrsta in obseg del, ki jih je treba opraviti.

(10) Pristojni nacionalni organ o ukrepih iz sedmega in devetega odstavka tega člena obvesti vlado in SNAV.

VIII. Kibernetska obramba

34. člen
(kibernetska obramba)

(1) Kibernetska obramba vključuje vse plasti kibernetskega prostora, in sicer družbeno, logično-tehnično in fizično. Pri tem:

- družbena plast zajema uporabnike medsebojno povezanih komunikacij, ki so lahko fizične ali pravne osebe, kot tudi njihove virtualne identitete;
- logično-tehnična plast zajema digitalne podatke, iz tretje alineje 27. točke 5. člena tega zakona;
- fizična plast zajema omrežja in naprave iz prve in druge alineje 27. točke 5. člena tega zakona.

(2) Z namenom preprečevanja kibernetskih groženj in incidentov v kibernetskem prostoru in za ublažitev njihovih učinkov se izvajajo ukrepi in dejavnosti ter gradijo zmogljivosti kibernetske obrambe.

35. člen
(kibernetska obramba na ravni državnih organov)

(1) Ukrepe in dejavnosti kibernetske obrambe na ravni državnih organov usklajujejo in izvajajo pristojni nacionalni organ, skupine CSIRT ter ministrstvo, pristojno za obrambo, ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, ministrstvo, pristojno za zunanje zadeve, ministrstvo, pristojno za notranje zadeve, policija, Slovenska obveščevalno-varnostna agencija (v nadaljnjem besedilu: SOVA) in drugi nacionalni organi v skladu s svojimi pristojnostmi pri zagotavljanju nacionalne varnosti. Na različnih ravneh izvajajo usklajene organizacijske, logično-tehnične, tehnične in administrativne ukrepe ter dejavnosti za zagotavljanje celovite kibernetske varnosti skladno s svojimi pristojnostmi. Koordinacijo kibernetske obrambe na ravni državnih organov izvaja pristojni nacionalni organ. V ta namen vzpostavi koordinacijsko skupino.

(2) Organi iz prejšnjega odstavka zagotavljajo ustrezne zmogljivosti za kibernetsko obrambo na področjih, za katere so pristojni. V ta namen lahko vzpostavijo svoje varnostno operativne centre organov državne uprave, ki izpolnjujejo vsaj minimalni obseg zahtev:

- stalno zagotavljanje razpoložljivosti svojih komunikacijskih kanalov;
- prostori in podporni informacijski sistemi se nahajajo na varnih krajih ter so odporni na okoljske vplive;
- zagotovijo zaupnost in zanesljivost svojih dejavnosti;
- imajo dovolj osebja za zagotavljanje neprekinjene razpoložljivosti storitev, pri čemer zagotavljajo, da je to osebje ustrezno usposobljeno;
- imajo redundantne sisteme in nadomestni delovni prostor, da se zagotovi neprekinjeno izvajanje njihovih storitev.

(3) Pristojni nacionalni organ, ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za zunanje zadeve, ter policija in SOVA stalno spremljajo stanje in odzive na dogodke v kibernetskem prostoru na področju njihovega delovanja.

(4) Pristojni organi iz prvega odstavka tega člena vzpostavitev varnostno operativnega centra organa državne uprave priglasijo pristojnemu nacionalnem organu v roku 30 dni od njegove vzpostavitve in hkrati predložijo izjavo o izpolnjevanju zahtev iz drugega odstavka tega člena.

(5) Namen izvajanja kibernetske obrambe iz prvega odstavka tega člena se uresničuje tudi z vključevanjem organov in skupin CSIRT iz tega člena v mednarodne povezave in njihovim aktivnim sodelovanjem v teh povezavah ter prek drugih oblik multilateralnega in bilateralnega sodelovanja.

(6) Varnostno operativni centri organov državne uprave pristojnemu nacionalnemu organu posredujejo tedensko in letno poročilo o izvajanju svojih nalog. Poročilo obsega informacijo o vseh zaznanih incidentih, kot tudi pomembnih incidentih, ki so jih priglasili CSIRT državne uprave.

(7) Osebam iz tretjega člena Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-1O) pristojni nacionalni organ omogoči seznanitev z osnovami kibernetske varnosti s kibernetsko higieno v treh mesecih od nastopa funkcije. Organ funkcionarja o novem funkcionarju, njegovih kontaktnih podatkih in datumu nastopa funkcije obvesti pristojni nacionalni organ v petnajstih dneh od nastopa funkcije.

36. člen
(sodelovanje na področju kibernetske obrambe)

(1) Za namen kibernetske obrambe pristojni nacionalni organ lahko sklene sporazume o sodelovanju, v katere se po potrebi vključi državne organe, organe lokalne samouprave, gospodarske družbe, zavode in druge organizacije.

(2) Pristojni nacionalni organ lahko za namen izvajanja kibernetske obrambe k sodelovanju povabi tudi državljane in državljanke (v nadaljnjem besedilu prostovoljci), ki:

- so državljani Republike Slovenije;
- so poslovno sposobni;
- so stari najmanj 18 let;
- ne smejo biti pravnomočno obsojeni zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, in ne smejo biti obsojeni na nepogojno kazen zapora v trajanju več kot šest mesecev oziroma ne smejo biti pravnomočno obsojeni za kazniva dejanja iz 221. in 237. člena Kazenskega zakonika (Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23);
- zoper njih ne sme biti vložena pravnomočna obtožnica zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti oziroma ni bil zoper njih uveden kazenski postopek zaradi suma storitve kaznivega dejanja iz 221. in 237. člena Kazenskega zakonika (Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23);
- soglasje delodajalca prostovoljca, v kolikor ta obstaja;
- imajo ustrezna znanja in kompetence za izvajanje nalog s področja kibernetske obrambe in
- se strinjajo z njihovim varnostnim preverjanjem po zakonu, ki ureja tajne podatke.

Vabilo k sodelovanju se objavi na spletni strani pristojnega nacionalnega organa.

(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.

(4) Prostovoljcu iz seznama iz prejšnjega odstavka pristojni nacionalni organ ponudi sklenitev pogodbenega razmerja, v katerem se uredi status, medsebojne pravice in dolžnosti ter nagrado prostovoljca. Pristojni nacionalni organ po sklenitvi pogodbenega razmerja za prostovoljce organizira priprave, dodatna usposabljanja in vaje za njihovo delovanje na področju kibernetske obrambe.

(5) Pristojni nacionalni organ oblikuje glede na potrebe in stanje ogroženosti kibernetske varnosti eno ali več operativnih skupin za kibernetsko obrambo, v katere vključi prostovoljce, s katerimi ima sklenjeno pogodbo iz prejšnjega odstavka tega člena in predstavnike državnih organov, organov lokalne samouprave, gospodarskih družb, zavodov in drugih organizacij, ki so svoje sodelovanje izrazile s sporazumom iz prvega odstavka tega člena.

(6) Direktor pristojnega nacionalnega organa imenuje vodjo in namestnika posamezne operativne skupine iz prejšnjega odstavka. V primeru, da se za vodjo ali namestnika imenuje osebo državnega organa, ki ni uslužbenec pristojnega nacionalnega organa, se zagotovi soglasje njegovega predstojnika. Administrativno-tehnične pogoje za delovanje operativnih skupin iz prejšnjega odstavka zagotovi pristojni nacionalni organ.

37. člen
(pomoč na področju kibernetske obrambe)

(1) Pristojni nacionalni organ lahko nudi zavezancem dodatno pomoč na področju kibernetske obrambe v primeru kibernetskih groženj in incidentov, o katerih pristojni nacionalni organ obvešča vlado in SNAV v skladu s tem zakonom, kot tudi v primeru kibernetskih incidentov velikih razsežnosti ali kriz.

(2) Zavezanec iz tega zakona ali pristojna skupina CSIRT lahko pristojni nacionalni organ zaprosijo za dodatno pomoč iz prejšnjega odstavka, pri čemer se v prošnji navedejo okoliščine, zaradi katerih se prosi za pomoč. Nudenje dodatne pomoči v vsakem posamičnem primeru odobri direktor pristojnega nacionalnega organa, pri čemer upošteva vidike nujnosti obvladovanja stanja ali dogodkov iz prejšnjega odstavka, razpoložljivosti operativnih skupin in drugih zmogljivosti za izvajanje kibernetske obrambe ter aktualno oceno kibernetske varnosti v državi. O načinu in pravilih nudenja dodatne pomoči, vključno glede možnosti vključitve operativnih skupin iz prejšnjega člena, se na operativni ravni uskladijo pristojni nacionalni organ, pristojna skupina CSIRT in zavezanec, pri čemer upoštevata tudi pravila, ki jih določa nacionalni načrt odzivanja.

(3) O tem, da pomoč iz prejšnjega odstavka ni bila odobrena, pristojni nacionalni organ le seznani prosilca iz prejšnjega odstavka, ki lahko v primeru spremenjenih okoliščin ponovno zaprosi za pomoč.

38. člen
(pomoč pri kibernetski obrambi znotraj Evropske unije)

(1) Republika Slovenija lahko zaprosi za pomoč pri izvajanju kibernetske obrambe druge države članice Evropske unije oziroma ustrezne institucije, organe, urade in agencij Evropske unije. Republika Slovenija lahko prej navedenim subjektom tudi nudi pomoč pri izvajanju kibernetske obrambe.

(2) Če pristojni nacionalni organ, zaradi obvladovanja stanja ali dogodkov iz prvega odstavka prejšnjega člena tega zakona, oceni, da zavezanci iz tega zakona ali pristojna skupina CSIRT potrebuje pomoč druge države ali držav članic Evropske unije pri kibernetski obrambi Republike Slovenije, o tem nemudoma obvesti SNAV, ki o predlogu zaprosila oblikuje stališče in ga posreduje vladi v odločanje. Medsebojni dogovor o pomoči določi tudi kritje morebitnih stroškov obeh strani, pri čemer morebitne stroške na strani Republike Slovenije krije prejemnik pomoči.

(3) O prejemu zaprosila pristojnih institucij ali organov druge države ali držav članic Evropske unije za nudenje pomoči pri kibernetski obrambi, pristojni nacionalni organ obvesti SNAV, ki o predlogu odziva na takšno zaprosilo oblikuje stališče in ga posreduje v odločanje vladi. Pri odzivu na zaprosilo se upošteva razpoložljivost zmogljivosti za kibernetsko obrambo ter aktualno oceno kibernetske varnosti v državi. Medsebojni dogovor o pomoči določi tudi kritje morebitnih stroškov obeh strani, pri čemer morebitne stroške na strani Republike Slovenije zagotovi organ, iz katerega izhaja oseba, ki je napotena, da nudi pomoč oziroma je za njih pristojna.

39. člen
(pomoč pri kibernetski obrambi na mednarodni ravni)

(1) Republika Slovenija lahko zaprosi za pomoč pri izvajanju kibernetske obrambe tudi tretje države ali mednarodne organizacije, s katerimi ima sklenjene mednarodne sporazume. Republika Slovenija lahko prej navedenim subjektom tudi nudi pomoč pri izvajanju kibernetske obrambe.

(2) Za nudenje in prejem pomoči se smiselno uporabljajo določbe prejšnjega člena.

(3) Republika Slovenija lahko sodeluje v skupnih enotah za kibernetsko obrambo, ki jih vzpostavijo mednarodne organizacije, katerih članica je. Odločitev o takšnem sodelovanju, na predlog SNAV, sprejme vlada.

40. člen
(delo v manj ugodnem delovnem času)

(1) Uslužbenci državnih organov, ki izvajajo kibernetsko obrambo morajo opravljati delo tudi v manj ugodnem delovnem času, kadar je to potrebno za izvajanje z zakonom določenih nalog.

(2) Delo v manj ugodnem delovnem času je:
1. delo v neenakomerno razporejenem delovnem času,
2. delo v izmenah,
3. delo ob sobotah, nedeljah, praznikih in drugih dela prostih dnevih,
4. delo preko polnega delovnega časa,
5. popoldansko in nočno delo,
6. delo v deljenem delovnem času.

(3) Delo v neenakomerno razporejenem delovnem času oziroma v izmenah vključuje opravljanje delovne obveznosti ob sobotah, nedeljah, praznikih in drugih dela prostih dnevih ter delo v popoldanskem in nočnem času s prerazporeditvijo delovnega časa v okviru določene redne mesečne oziroma letne delovne obveznosti.

(4) Delovna mesta, na katerih poteka delo v skladu s prejšnjim odstavkom, se določijo v aktu o organizaciji in sistemizaciji.

(5) Če to terjajo varnostne razmere oziroma če je samo tako mogoče opraviti določene naloge, ki jih ni mogoče odlagati ali pa morajo biti opravljene v določenem roku, se lahko odredijo tudi druge oblike dela, kot so določene v drugem odstavku tega člena.

(6) Predstojnik državnega organa določi primere, v katerih je dovoljeno odrediti delo iz prejšnjega odstavka, in osebe, ki ga lahko odredijo.

IX. Nadzor

41. 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).

(2) Inšpektor je pristojen tudi za nadzor nad izvajanjem določb Uredbe (EU) 2019/881 in evropskimi certifikacijskimi shemami ter nad izvršitvijo upravnih odločb, ki jih izda nacionalni certifikacijski organ za kibernetsko varnost na podlagi sedmega ali osmega odstavka 23. člena tega zakona.

(3) V postopku nadzora po tem zakonu se uporabljajo določbe zakona, ki ureja inšpekcijski nadzor, če s tem zakonom ni določeno drugače.

(4) Inšpektor nadzira ali zavezanci izpolnjujejo svoje obveznosti iz tega zakona predvsem z neposrednim vpogledom v podatke, dokumentacijo ter v omrežne in informacijske sisteme; preverjanjem pogojev in načina izvajanja ukrepov za obvladovanje tveganj kibernetske varnosti; pregledom območij, objektov in prostorov zavezancev, kjer se nahajajo ključni, krmilni in nadzorni informacijski sistemi ter podatki, pregledom dokumentacije o izvrševanju predpisanih obveznosti obveščanja o kibernetskih incidentih ter drugih obveznostih na podlagi zahtev pristojnih organov iz tega zakona; pregledom poročil o izvedbi revizije informacijskih sistemov in varnostnih pregledov omrežja ter informacijskih sistemov in pregledom druge dokumentacije, potrebne za izvedbo nadzora.

(5) Zavezanci morajo inšpektorju, pri izvajanju inšpekcijskega nadzora, brez odlašanja posredovati zahtevane informacije in podatke ter omogočiti dostop do sistemov, območij, objektov in prostorov.

(6) Zoper odločbo, izdano v postopkih nadzora po tem zakonu, ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu Upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.

(7) Inšpektor lahko v inšpekcijskem postopku na podlagi obrazloženega predloga zavezanca za podaljšanje rokov za odpravo nepravilnosti in pomanjkljivosti, ki je podan pred potekom roka za izvedbo odrejenih ukrepov, podaljša roke za odpravo nepravilnosti in pomanjkljivosti oziroma izvedbo odrejenih ukrepov, pri tem pa upošteva že izvedene aktivnosti zavezanca

za odpravo nepravilnosti in pomanjkljivosti, objektivne okoliščine za zamudo in posledice za javni interes.

(8) Inšpektor lahko poleg ukrepov, ki določa zakon, ki ureja inšpekcijski nadzor, odredi tudi ukrepe, določene s tem zakonom ali ukrepe določene z Uredbo (EU) 2019/881

(9) Inšpektor utemelji odrejene ukrepe v okviru izvedbe inšpekcijskega nadzora. Pred sprejetjem teh ukrepov zadevne zavezance obvesti o svojih predhodnih ugotovitvah in jim da na voljo dovolj časa za predložitev pripomb, razen v ustrezno utemeljenih primerih, ko bi to oviralo takojšnje ukrepanje za preprečitev incidentov ali odziv nanje.

(10) Inšpektor lahko določi prednostno razvrščanje izvedbe nadzorov zavezancev po tem zakonu. Pri določanju tega se upošteva pristop, ki temelji na tveganjih. S tem namenom inšpektor lahko določi tudi metodologijo za prednostno razvrščanje izvedbe nadzorov.

42. člen
(nadzor bistvenih subjektov)

(1) Inšpektor ima pri izvajanju svojih nadzornih nalog pri bistvenih subjektih, poleg pooblastil, ki jih določa zakon, ki ureja inšpekcijski nadzor, tudi pravico:

1. opraviti inšpekcijske preglede na kraju samem in nadzor na daljavo, vključno z naključnimi pregledi, ki jih lahko izvede skupaj z usposobljenimi strokovnjaki;
2. odrediti izvedbo redne in ciljno usmerjene revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti, ki jo izvede preizkušeni revizor informacijskih sistemov;
3. odrediti izvedbo izredne revizije skladnosti, ki jo izvede preizkušeni revizor informacijskih sistemov, ko je to utemeljeno zaradi pomembnega incidenta ali očitne kršitve tega zakona s strani bistvenega subjekta;
4. opraviti varnostni pregled, ki temelji na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganj;
5. odrediti zavezancu, da obvesti fizične ali pravne osebe, v zvezi s katerimi opravlja storitve ali izvaja dejavnost, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;
6. odrediti, da zavezanec v razumnem roku izvede priporočila, dana na podlagi izvedene revizije skladnosti;
7. imenovati pooblaščeno osebo z natančno opredeljenimi nalogami v določenem obdobju, ki spremlja izpolnjevanje določb 20., 21, 25. in 26. člena tega zakona s strani bistvenega subjekta;
8. odrediti zavezancu, da na določen način objavi kršitve tega zakona.

(2) Če inšpektor ugotovi, da odrejeni ukrepi za odpravo nepravilnosti oziroma pomanjkljivosti niso bili učinkoviti, bistvenemu subjektu, ki ga takšni ukrepi zadevajo, določi rok, v katerem mora sprejeti potrebne ukrepe za odpravo nepravilnosti oziroma pomanjkljivosti ali izpolnitev zahtev inšpektorja. Če bistveni subjekt ukrepov ne sprejme v določenem roku, inšpektor z odločbo lahko:

1. začasno prekliče certifikat ali dovoljenje za del ustreznih storitev ali začasno prepove izvajanje dejavnosti ali vse storitve ali dejavnosti, ki jih opravlja bistveni subjekt;
2. zahteva, začasno prepoved opravljanja vodstvenih funkcij vsem osebam, ki za bistveni subjekt opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika.

(3) Začasni preklic ali prepoved, naložena na podlagi prejšnjega odstavka, se uporabljata samo, dokler zadevni bistveni subjekt ne sprejme potrebnih ukrepov za odpravo pomanjkljivosti ali ne izpolni zahtev inšpektorja, zaradi katerih je bil tak ukrep uporabljen.

(4) Ukrepi iz drugega odstavka tega člena se ne uporabljajo za subjekte javne uprave, za katere velja ta zakon.

(5) Inšpektor pri sprejemanju ukrepov iz prvega in drugega odstavka tega člena spoštuje postopkovne pravice bistvenega subjekta v postopku nadzora in upošteva okoliščine vsakega posameznega primera pri čemer ustrezno upošteva vsaj:

1. resnost kršitve in pomembnost kršenih določb, pri čemer se za resne kršitve v vsakem primeru štejejo:
   - ponavljajoče se kršitve;
   - nepriglasitev ali neodprava pomembnih incidentov;
   - neodprava pomanjkljivosti v skladu z zavezujočimi navodili inšpektorja;
   - oviranje revizij ali dejavnosti spremljanja, ki jih je odredil inšpektor po ugotovitvi kršitve;
   - predložitev napačnih ali zelo netočnih informacij v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost ali obveznostmi poročanja iz 20., 21., 25. ali 26. člena tega zakona;
2. trajanje kršitve;
3. vse relevantne prejšnje kršitve zadevnega bistvenega subjekta;
4. morebitno povzročeno premoženjsko ali nepremoženjsko škodo, vključno s finančnimi ali gospodarskimi izgubami, učinki na druge storitve in številom prizadetih uporabnikov;
5. morebitni naklep ali malomarnost storilca kršitve;
6. morebitne ukrepe, ki jih je bistveni subjekt sprejel za preprečevanje ali zmanjšanje premoženjske ali nepremoženjske škode;
7. morebitno upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja;
8. raven sodelovanja odgovornih fizičnih ali pravnih oseb z inšpektorjem.

(6) 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.

(7) Ciljno usmerjene revizije skladnosti iz 2. točke prvega odstavka tega člena temeljijo na ocenah tveganj, ki jih izvedejo pristojni nacionalni organi ali bistveni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Poročilo o izvedeni ciljno usmerjeni reviziji varnosti se da na voljo inšpektorju.

(8) Stroške redne, izredne ali ciljno usmerjene revizije skladnosti, ki jo opravi preizkušeni revizor informacijskih sistemov, krije bistven subjekt, razen v ustrezno utemeljenih primerih, ko pristojni organ odloči drugače.

(9) Inšpektor pri izvajanju svojih pooblastil navede namen zahteve in opredeli zahtevane informacije. Pri odreditvi izredne revizije skladnosti iz 3. točke prvega odstavka tega člena inšpektor določi obseg revizije.

(10) Inšpektor obvesti pristojno inšpekcijo za področje kritične infrastrukture, kadar izvaja nadzor nad subjektom, ki je na podlagi zakona, ki ureja kritično infrastrukturo določen kot kritičen. Inšpektor za področje kritične infrastrukture lahko kadar oceni, da je to utemeljeno, tudi sam poda pobudo Inšpekciji za informacijsko varnost, da izvede nadzor v zvezi s subjektom, ki je na podlagi zakona identificiran kot kritičen.

(11) Inšpektor sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554. Pri tem inšpektor zagotovi, da o nadzoru bistvenega 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.

(12) Kadar inšpektor opravlja upravno izvršbo izvršljivih odločb, ki jih je izdal v postopku nadzora bistvenih subjektov in pri tem uporablja prisilne ukrepe z izrekanjem denarnih kazni, pri tem prva denarna kazen ne glede na zakon, ki ureja splošni upravni postopek, ne sme presegati 10.000,00 evrov. Vsaka poznejša denarna kazen za prisilitev je lahko znova izrečena do tega zneska.

(13) Določbe prejšnjega odstavka se ne uporabljajo za pravne osebe javnega prava, za njihove odgovorne osebe pa se za prisilne ukrepe z izrekanjem denarnih kazni uporabljajo določbe zakona o splošnem upravnem postopku.

(14) Predstojnik organa subjekta javne uprave ali odgovorna oseba pravne osebe, ki je bistven subjekt ali deluje kot njen zastopnik na podlagi pooblastila za njegovo zastopanje oziroma odločanje v njegovem imenu je odgovorna oseba za zagotavljanje skladnosti delovanja bistvenega subjekta po tem zakonu (v nadaljnjem besedilu odgovorna oseba bistvenega subjekta) in odgovarjajo za kršitve svojih dolžnosti v skladu s tem zakonom.

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.

(2) Inšpektor ima pri izvajanju svojih nadzornih nalog pri pomembnih subjektih, poleg pooblastil, ki jih določa zakon, ki ureja inšpekcijski nadzor, tudi pravico:

1. opraviti inšpekcijski pregled na kraju samem in nadzor na daljavo, ki ju lahko izvede skupaj z usposobljenimi strokovnjaki;
2. odrediti izvedbo ciljno usmerjene revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti, ki jo izvede preizkušeni revizor informacijskih sistemov;
3. opraviti varnostni pregled, ki temelji na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganj;
4. odrediti, da zavezanec obvesti fizične ali pravne osebe, za katere opravlja storitve ali izvaja dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe izvedejo v odziv na to grožnjo;
6. odrediti, da zavezanec v razumnem roku izvede priporočila, dana na podlagi ciljno usmerjene revizije skladnosti;
7. odrediti, da zavezanec na določen način objavi kršitve tega zakona.

(3) Inšpektor pri izvajanju ukrepov iz prejšnjega odstavka spoštuje postopkovne pravice pomembnega subjekta v postopku nadzora in upošteva okoliščine vsakega posameznega primera pri čemer upošteva:

1. resnost kršitve in pomembnost kršenih določb, pri čemer se za resne kršitve med drugim v vsakem primeru štejejo:
   - ponavljajoče se kršitve;
   - nepriglasitev ali neodprava pomembnih incidentov;
   - neodprava pomanjkljivosti v skladu z zavezujočimi navodili inšpektorja;
   - oviranje revizij ali dejavnosti spremljanja, ki jih je odredil inšpektor po ugotovitvi kršitve;
   - predložitev napačnih ali zelo netočnih informacij v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost ali obveznostmi poročanja iz 20., 21., 25. in 26. člena tega zakona;
2. trajanje kršitve;
3. vse relevantne prejšnje kršitve zadevnega pomembnega subjekta;
4. morebitno povzročeno premoženjsko ali nepremoženjsko škodo, vključno s finančnimi ali gospodarskimi izgubami, učinki na druge storitve in številom prizadetih uporabnikov;
5. morebitni naklep ali malomarnost storilca kršitve;
6. morebitne ukrepe, ki jih je pomembni subjekt sprejel za preprečevanje ali zmanjšanje premoženjske ali nepremoženjske škode;
7. morebitno upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja;
8. raven sodelovanja odgovornih fizičnih ali pravnih oseb z inšpektorjem.

(4) Ciljno usmerjene revizije skladnosti iz 2. točke prvega odstavka tega člena temeljijo na ocenah tveganj, ki jih izvedejo pristojni nacionalni organi ali pomembni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Poročilo o izvedeni ciljno usmerjeni reviziji skladnosti se da na voljo inšpektorju.

(5) Stroške ciljno usmerjene revizije skladnosti, ki jo opravi preizkušeni revizor informacijskih sistemov, krije pomemben subjekt, razen v ustrezno utemeljenih primerih, ko pristojni organ odloči drugače.

(6) Predstojnik organa subjekta javne uprave ali odgovorna oseba pravne osebe, ki je pomemben subjekt ali deluje kot njen zastopnik na podlagi pooblastila za njegovo zastopanje oziroma odločanje v njegovem imenu je odgovorna oseba za zagotavljanje skladnosti delovanja pomembnega subjekta po tem zakonu (v nadaljnjem besedilu odgovorna oseba pomembnega subjekta) in odgovarjajo za kršitve svojih dolžnosti v skladu s tem zakonom.

(7) Kadar inšpektor opravlja upravno izvršbo izvršljivih odločb, ki jih je izdal v postopku nadzora pomembnih subjektov in pri tem uporablja prisilne ukrepe z izrekanjem denarnih kazni prva, denarna kazen ne glede na zakon, ki ureja splošni upravni postopek, ne sme presegati 7.000,00 evrov. Vsaka poznejša denarna kazen za prisilitev je lahko znova izrečena do tega zneska.

(8) Določbe prejšnjega odstavka se ne uporabljajo za pravne osebe javnega prava, za njihove odgovorne osebe pa se za prisilne ukrepe z izrekanjem denarnih kazni uporabljajo določbe zakona o splošne upravnem postopku.

(9) 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.

44. člen
(nadzor subjektov po Uredbi (EU) 2019/881)

(1) Inšpekcijski nadzor subjektov po Uredbi (EU) 2019/881 se izvede, če inšpektor prejme dokaze, indice ali informacije, da organ za ugotavljanje skladnosti, imetnik evropskih certifikatov kibernetske varnosti ali izdajatelj izjav EU o skladnosti ne izpolnjuje zahtev iz Uredbe (EU) 2019/881 ali evropske certifikacijske sheme.

(2) Inšpektor ima pri izvajanju svojih nadzornih nalog subjektov po Uredbi (EU) 2019/881, poleg pooblastil, ki jih določa zakon, ki ureja inšpekcijski nadzor še pravico, da:

1. opravi inšpekcijski pregled na kraju samem in nadzor na daljavo, ki ju lahko izvede skupaj z usposobljenimi strokovnjaki;
2. odredi izvedbo ciljno usmerjene revizije skladnosti z Uredbo (EU) 2019/881, ki jo izvede preizkušeni revizor informacijskih sistemov;
4. odredi izvedbo ustreznih ukrepov, da se zagotovi izpolnjevanje zahtev iz Uredbe (EU) 2019/881 ali evropske certifikacijske sheme;
5. predlaga nacionalnemu certifikacijskemu organi za kibernetsko varnost odvzem evropskega certifikata kibernetske varnosti, kadar taki certifikati niso skladni s to uredbo ali z evropsko certifikacijsko shemo.

(3) Poročilo o izvedeni ciljno usmerjeni reviziji skladnosti iz 2. točke prejšnjega odstavka se da na voljo inšpektorju.

(4) Stroške ciljno usmerjene revizije skladnosti, ki jo opravi preizkušeni revizor informacijskih sistemov, krije subjekt iz prvega odstavka tega člena.

(5) Inšpektor pri izvajanju svojih pooblastil navede namen zahteve in opredeli zahtevane informacije. Pri odreditvi ciljno usmerjene revizije skladnosti inšpektor določi obseg revizije.

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 skladnosti s predpisi s področja informacijske varnosti ali v okviru notranje revizije, 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. Oceno skladnosti v okviru notranje revizije poleg preizkušenih revizorjev lahko izvajajo tudi notranji revizorji v sodelovanju z veščakom za informacijsko tehnologijo.

(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.

(5) Bistveni in pomembni subjekti morajo poročilo iz prejšnjega odstavka tega člena posredovati inšpektorju v osmih dneh po njegovem prejemu.

(6) Ne glede na določbe prejšnjega odstavka tega člena, kadar se ugotavljanje skladnosti izvaja na zahtevo inšpektorja, na podlagi drugega ali tretjega tega člena mora subjekt, kjer se je ocena skladnosti opravila, poročilo iz prejšnjega odstavka predloži inšpektorju nemudoma po prejemu.

(7) Stroške izvedbe ocene skladnosti nosijo bistveni in pomembni subjekti, če ta zakon ne določa drugače.

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.

47. člen
(določitev preizkušenega revizorja)

(1) Bistveni ali pomembni subjekt za izvedbo revizije skladnosti, ki jo zahteva inšpektor po tem zakonu, izbere preizkušenega revizorja. O svoji izbiri in o začetku postopka revizije skladnosti s predpisi s področja informacijske varnosti obvesti inšpektorja v roku 30 dni od podane zahteve inšpektorja.

(2) Če bistveni ali pomembni subjekt ne izbere preizkušenega revizorja v skladu s prejšnjim odstavkom tega s sklepom določi inšpektor.

48. člen
(kršitve, ki pomenijo kršitev 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.

(2) Kadar Informacijski pooblaščenec zaradi kršitve določbe točka (i) drugega odstavka 58. člena Uredbe (EU) 2016/679 naloži globo na podlagi zakona, ki ureja varstvo osebnih podatkov. Inšpektor poleg ukrepov nadzora, določenih določbah 1. do 8. točk prvega odstavka in drugega odstavka 42. člena tega zakona ter določb 1. do 7. točk prvega odstavka 44. člena ne naloži globe za kršitev tega zakona zaradi istega ravnanja, zaradi katerega je Informacijski pooblaščenec naložil grobo zaradi prej navedene kršitve.

(3). Kadar ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679, sedež v drugi državi članici kot inšpektor, inšpektor obvesti Informacijskega pooblaščenca, o možni kršitvi varstva osebnih podatkov iz prvega odstavka tega člena.

49. člen
(medsebojna pomoč in čezmejni nadzor)

(1) Kadar bistveni ali pomembni subjekt spada v pristojnost pristojnega nacionalnega organa v skladu s 27. členom tega zakona, vendar opravlja storitve v več kot eni državi članici Evropske unije ali opravlja storitve v eni ali več državah članicah Evropske unije, njegovi omrežni in informacijski sistemi pa se nahajajo v drugi državi članici Evropske unije oziroma v več kot eni državi članici Evropske unije, inšpektor lahko izvaja inšpekcijski nadzor nad temi subjekti v sodelovanju s pristojnimi organi nadzora zadevnih drugih držav članic Evropske unije. Inšpektor in pristojni organi nadzora drugih držav članic Evropske unije si medsebojno pomagajo pri izvajanju takega nadzora.

(2) Za izvajanje medsebojne pomoči iz prejšnjega odstavka inšpektor preko enotne kontaktne točke najmanj:

- obvešča pristojne organe nadzora v drugih državah članicah Evropske unije o svojih sprejetih nadzornih ukrepih in izrečenih ukrepih za odpravo nepravilnosti;
- lahko zahteva izvedbo nadzornih ukrepov ali izrek ukrepov za odpravo nepravilnosti od pristojnega organa nadzora v drugi državi članici Evropske unije;
- zahteva od pristojnega organa nadzora druge države članice Evropske unije ali pa le-temu na obrazloženo zahtevo zagotovi sorazmerno medsebojno pomoč, oboje z namenom, da se nadzorni ukrepi oziroma izrečeni popravljalni ukrepi izvedejo učinkovito, uspešno in dosledno.

(3) Zahteva za medsebojna pomoč iz zadnje alineje prejšnjega odstavka lahko vključuje zahtevke za posredovanje ustreznih informacij in za izvajanje nadzornih ukrepov, vključno z zahtevki za izvajanje inšpekcijskih pregledov na kraju samem ali nadzora na daljavo ali za ciljno usmerjene varnostne presoje.

(4) Inšpektor, ki mu je bila poslana zahteva pristojnega organa nadzora druge države članice Evropske unije za medsebojno pomoč pri izvajanju inšpekcijskega nadzora iz prvega odstavka tega člena, izvedbe takšne prejete zahteve ne sme zavrniti, razen v primeru, ko ugotovi, da:

- ni pristojen za zagotavljanje zahtevane medsebojne pomoči;
- da zahtevana medsebojna pomoč ni sorazmerna s pristojnostmi inšpektorja po tem zakonu in
- da se zahteva nanaša na podatke ali dejavnosti, ki bi bile v primeru njihovega razkritja ali izvajanja v nasprotju z interesi nacionalne varnosti, javne varnosti ali obrambe.

(5) Pred zavrnitvijo zahteve iz prejšnjega odstavka se inšpektor posvetuje z drugimi pristojnim organi nadzora držav članic Evropske unije, ki so tudi pristojne za obravnavo nadzora v konkretnem primeru. V primeru, da druga država članica Evropske unije, v katere pristojnost tudi sodi obravnava zadevnega postopka nadzora, tako zahteva, se mora inšpektor pred zavrnitvijo zahteve za medsebojno pomoč predhodno posvetovati tudi z Evropsko komisijo in ENISA.

(6) V primerih iz prvega odstavka tega člena, se na podlagi in v okviru skupnega dogovora inšpektorja z za takšen nadzor pristojnimi organi drugih držav članic Evropske unije, lahko izvaja skupni inšpekcijski nadzor.

50. člen
(določanje glob v posebnih primerih)

(1) Poleg splošnih pravil za odmero sankcije iz zakona, ki ureja prekrške, se pri odločanju o višini izrečene globe za kršitve določb 20., 21., 25. ali 26. člena tega zakona s strani bistvenih subjektov in pomembnih subjektov upošteva tudi letni promet oziroma letna bilančna vsota bistvenega ali pomembnega subjekta v predhodnem poslovnem letu.

(2) V primerih iz prejšnjega odstavka se bistvenim subjektom, ki so srednja ali velika podjetja, lahko izreče globa v višini do dveh odstotkov letnega prometa podjetja v predhodnem poslovnem letu, če je prekršek storjen naklepno ali iz malomarnosti. Tako določena globa ne sme biti višja od 10.000.000,00 eurov.

(3) V primerih iz prvega odstavka tega člena se pomembnim subjektom, ki so srednja ali velika podjetja, lahko izreče globa v višini do 1,4 odstotka letnega prometa podjetja v predhodnem poslovnem letu, če je prekršek storjen naklepno ali iz malomarnosti. Tako določena globa ne sme biti višja od 7.000.000,00 eurov.

(4) Pri določanju o naložitvi in višini višine globe iz tega člena se upoštevajo okoliščine posameznega primera in vsaj elementi določeni v prvem odstavku 42. člena tega zakona.

51. člen
(izrekanje globe v hitrem prekrškovnem postopku)

Za prekrške iz tega zakona se sme v hitrem prekrškovnem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom.

52. člen
(uporaba določb o prekrških)

Do sprememb določb o višinah in razponih glob, ki jih določa zakon, ki ureja prekrške, se višine in razponi glob, določeni v 50. členu tega zakona, uporabljajo ne glede na določbe zakona, ki ureja prekrške.

X. Kazenske določbe

53. člen
(prekrški bistvenih subjektov)

(1) Z globo od 10.000,00 eurov do 10.000.000,00 eurov oziroma v višini od 0,5 % do 2 % skupnega letnega prometa pravne osebe, doseženega v preteklem poslovnem letu, odvisno od tega, kateri znesek je višji, se kaznuje pravna oseba, če:

- ne izpolni obveznosti iz 20. člena tega zakona;
- ne izpolni obveznosti iz 21. člen tega zakona;
- ne izpolni obveznosti iz 25. člena tega zakona;

- ne izpolni obveznosti iz prvega ali drugega odstavka 26. člena tega zakona.

(2) Z globo od 5.000,00 eurov do 25.000,00 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če stori prekršek iz prejšnjega odstavka.

(3) Z globo od 1.000,00 eurov do 10.000,00 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, če stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 3.000,00 eurov do 15.000,00 eurov, se kaznuje pravna oseba, če:
- ne izpolni obveznosti iz drugega in 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 štirinajstega 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 46. člena tega zakona.

(5) Z globo od 1.000,00 eurov do 10.000,00 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če ne izpolni obveznosti iz prejšnjega odstavka tega člena.

(6) Z globo od 500,00 eurov do 3.000,00 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, če ne izpolni obveznosti iz četrtega odstavka tega člena.

54. člen
(prekrški pomembnih subjektov)

(1) Z globo od 7.000,00 eurov do 7.000.000,00 eurov oziroma v višini od 0,3 % do 1,4 % skupnega letnega prometa pravne osebe, doseženega v preteklem poslovnem letu, odvisno od tega, kateri znesek je višji, se kaznuje pravna oseba, če:
- ne izpolni obveznosti iz 20. člena tega zakona;
- ne izpolni obveznosti iz 21. člen tega zakona;
- ne izpolni obveznosti iz 25. člena tega zakona;
- ne izpolni obveznosti iz prvega ali drugega odstavka 26. člena tega zakona.

(2) Z globo od 3.000,00 eurov do 20.000,00 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost in je pomemben subjekt po tem zakonu, če stori prekršek iz prejšnjega odstavka.

(3) Z globo od 1.000,00 eurov do 7.000,00 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu,

samoupravni lokalni skupnosti ali v drugi osebi javnega prava, ki je pomemben subjekt po tem zakonu, če stori prekršek iz prvega odstavka tega člena.

(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 štirinajstega 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 46. člena tega zakona.

(5) Z globo od 500,00 eurov do 7.000,00 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če ne izpolni obveznosti iz prejšnjega odstavka tega člena.

(6) Z globo od 200,00 eurov do 2.000,00 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, če ne izpolni obveznosti iz četrtega odstavka tega člena.

55. člen
(prekrški upravljavca centralnega informacijsko-komunikacijskega sistema)

(1) Z globo od 200,00 eurov do 2.000,00 eurov se za prekršek kaznuje odgovorna oseba upravljavca centralnega informacijsko-komunikacijskega sistema, če:
- ne omogoča vpogleda v delovanje informacijske infrastrukture centralnega informacijsko-komunikacijskega sistema za CSIRT državne uprave (sedmi odstavek 14. člena tega zakona),
- ne izvede odrejenih ukrepov CSIRT državne uprave v svojem informacijsko-komunikacijskem sistemu (osmi odstavek 14. člena tega zakona).

56. člen
(prekrški za kršitev Uredbe (EU) 2019/881)

(1) Z globo od 5.000,00 do 50.000,00 eurov se kaznuje za prekršek proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT iz člena 53 Uredbe (EU) 2019/881, ki po izvedenem postopku samoocenjevanja skladnosti izda izjavo EU o skladnosti za proizvod IKT, storitev IKT ali postopek IKT, ki ustreza »osnovni« ravni zanesljivosti, čeprav proizvod IKT, storitev IKT ali postopek IKT ne izpolnjuje zahteve iz certifikacijske sheme.

(2) Z globo od 1.000,00 eurov do 10.000,00 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki je proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT iz člena 53 Uredbe (EU) 2019/881, če stori prekršek iz prejšnjega odstavka.

(3) Z globo od 500,00 eurov do 5.000,00 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, ki je proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT iz člena 53 Uredbe (EU) 2019/881, če stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 3.000,00 do 20.000,00 eurov se kaznuje za prekršek proizvajalec ali ponudnik certificiranih proizvodov IKT, storitev IKT in postopkov IKT ali proizvodov IKT, storitev IKT in postopkov IKT, za katere je bila izdala izjava EU o skladnosti iz člena 55 Uredbe (EU) 2019/881, ki:

- ne da na voljo dodatnih informacij o kibernetski varnosti iz 1. točke člena 55 Uredbe (EU) 2019/881 ali so te informacije nepopolne ali zavajajoče,
- pred iztekom veljavnosti ustreznega evropskega certifikata kibernetske varnosti ali izjave EU o skladnosti onemogoči dostop do dodatnih informacij o kibernetski varnosti iz 1. točke člena 55 Uredbe (EU) 2019/881 ali jih ne posodablja.

(5) Z globo od 500,00 eurov do 7.000,00 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki je proizvajalec ali ponudnik certificiranih proizvodov IKT, storitev IKT in postopkov IKT ali proizvodov IKT, storitev IKT in postopkov IKT, za katere je bila izdala izjava EU o skladnosti iz člena 55 Uredbe (EU) 2019/881, če stori prekršek iz prejšnjega odstavka.

(6) Z globo od 500,00 eurov do 2.000,00 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, ki je proizvajalec ali ponudnik certificiranih proizvodov IKT, storitev IKT in postopkov IKT ali proizvodov IKT, storitev IKT in postopkov IKT, za katere je bila izdala izjava EU o skladnosti iz člena 55 Uredbe (EU) 2019/881, če stori prekršek iz četrtega odstavka tega člena.

XI. Prehodne določbe

57. 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.
(3) Organi iz devetega odstavka 7. člena tega zakona v roku iz prejšnje točke seznanijo pristojni nacionalni organ z identiteto subjektov in zahtevanimi vsebinami iz te določbe ob upoštevanju uveljavljenih področnih predpisov.
(4) Pristojni nacionalni organ vzpostavi prvi seznam iz četrtega odstavka 7. člena tega zakona v roku enega meseca po izteku roka iz prejšnjega odstavka.
(5) Pristojni nacionalni organ do 17. aprila 2025 prvič obvesti Evropsko komisijo in Skupino za sodelovanje o številu bistvenih in pomembnih subjektov, ki so na seznamu iz četrtega odstavka 7. člena tega zakona za vsak sektor in podsektor iz Priloge I ali II.

(6) Pristojni nacionalni organ v roku iz prejšnjega odstavka prvič obvesti Evropsko komisijo o ustreznih informacijah iz sedmega odstavka 7. člena tega zakona.
(7) Pristojni nacionalni organ o njegovi določitvi in nalogah prvič uradno obvesti Evropsko komisijo v skladu z 9. členom tega zakona v roku petnajstih dni od uveljavitve tega zakona.
(8) Pristojni nacionalni organ o določitvi enotne kontaktne točke v skladu z 10. členom tega zakona prvič uradno obvesti Evropsko komisijo v roku petnajstih dni od uveljavitve tega zakona.
(9) Pristojni nacionalni organ o določitvi organa za obvladovanje kibernetskih kriz v skladu z 11. členom tega zakona prvič uradno obvesti Evropsko komisijo v roku treh mesecev od uveljavitve tega zakona.
(10) Pristojni nacionalni organ o identiteti skupin CSIRT iz prvega odstavka 12 člena ter nalogah iz drugega in tretjega odstavka 12. člena prvič uradno obvesti Evropsko komisijo v roku petnajstih dni od uveljavitve tega zakona.
(11) Pristojni nacionalni organ vzpostavi digitalno platformo za medsebojno izmenjava informacij o relevantnih incidentih, kibernetskih grožnjah in skorajšnjih incidentih iz drugega odstavka 17. člena tega zakona v enem letu od uveljavitve tega zakona.
(12) Skupine CSIRT in pristojni nacionalni organ vzpostavi namensko digitalno platformo iz desetega odstavka 26. člena v enem letu od uveljavitve tega zakona.
(13) Subjekti iz prvega odstavka 28. člena tega zakona o informacijah iz navedene določbe prvič obvestijo pristojni nacionalni organ do 17. januarja 2025, ki te informacije brez nepotrebnega odlašanja prvič posreduje ENISA na način iz četrtega odstavka 28. člena tega zakona.
(14) Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen vzpostavijo politike in postopke iz tretjega in petega odstavka 29. člena v šestih mesecih od uveljavitve tega zakona.
(15) Organi iz prvega odstavka 35. člena tega zakona pristojni nacionalni organ obvestijo o obstoječih varnostno operativnih centrih organov državnih organov, ki izpolnjujejo zahteve iz drugega odstavka 35. člena v tridesetih dneh od uveljavitve tega zakona.
(16) Organi iz prvega odstavka 35. člena tega zakona pristojni nacionalni organ obvestijo o obstoječih varnostno operativnih centrih organov državne uprave, ki ne izpolnjujejo zahtev iz drugega odstavka 35. člena v tridesetih dneh od uveljavitve tega zakona, zagotovijo izpolnjevanje le-teh v enem letu od uveljavitve zakona.
(17) Pristojni nacionalni organ v teh mesecih od sprejetja nacionalnega načrta odzivanja iz četrtega odstavka 59. člena tega zakona predloži Evropski komisiji in mreži EU-CyCLONe ustrezne informacije v zvezi z zahtevami iz tretjega odstavka 11. člena tega zakona.

58. člen
(sprejem ukrepov za obvladovanje tveganj)

(1) Bistveni in pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost iz 20. in 21 člena tega zakona v roku dvanajstih mesecev od uveljavitve tega zakona.

(2) Ne glede na prejšnji odstavek v roku šestih mesecev od uveljavitve tega zakona sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost iz 20. in 21 člena tega zakona tisti bistveni ali pomembni subjekti:

- če so bili pred 16. januarjem 2023 določeni kot izvajalci bistvenih storitev, ponudniki bistvenih storitev ali organi državne uprave po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) ali

- operaterji po Zakonu o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O), ki in so vpisani v uradno evidenco, ki jo vodi Agencija za komunikacijska omrežja in storitve Republike Slovenije.

59. člen
(uskladitev obstoječe podatkovne zbirke o registraciji domenskih imen)

Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen uskladijo obstoječe podatkovne zbirke o registraciji domenskih imen z drugim in četrtim odstavkom 29. člena tega zakona za registracije, ki so bile izvedene do uveljavitve tega zakona v roku osemnajstih mesecev od uveljavitve tega zakona.

60. člen
(izdaja podzakonskih predpisov in strategije)

(1) Vlada izda predpise, ki so po tem zakonu obvezni, v enem letu od uveljavitve tega zakona.

(2) Vlada uskladi Odlok o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za informacijsko varnost (Uradni list RS, št. 114/21 in 69/23) s tem zakonom v treh mesecih od njegove uveljavitve.

(3) Vlada sprejeme strategijo iz 8. člena tega zakona v enem letu od uveljavitve tega zakona.

(4) Vlada sprejme nacionalni načrt odzivanja iz tretjega odstavka 11. člena tega zakona v roku treh mesecev od uveljavitve tega zakona.

(5) Vlada sprejme program usposabljanja odgovornih oseb iz šestega odstavka 19. člena tega zakona v roku šestih mesecev od uveljavitve tega zakona

61. člen
(prenehanje veljavnosti in podaljšanje uporabe)

(1) Z dnem uveljavitve tega zakona preneha veljati Zakon o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23).

(2) Z dnem uveljavitve tega zakona prenehajo veljati podzakonski predpisi, ki so bili izdani na podlagi zakona iz prejšnjega odstavka:

- Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev (Uradni list RS, št. 39/19);
- Uredba o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 8/23);
- Uredba o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 98/23);
- Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov (Uradni list RS, št. 118/23).

(3) Podzakonski predpisi iz prejšnjega odstavka se smiselno uporabljajo do izdaje podzakonskih predpisov sprejetih na podlagi tega zakona.

62. člen
(spremembe in dopolnitve Zakona o elektronskih komunikacijah)

(1) Z dnem uveljavitve tega zakona prenehajo veljati določbe 118., 119., 120., 121., 122. in 123. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O).

(2) V Zakonu o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O):

- besedilo 115. člena tega zakona se nadomesti z besedilom »Operaterji morajo sprejeti ustrezne in sorazmerne tehnične ter organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev, vključno s pripadajočimi informacijskimi sistemi, v skladu z zakonom, ki ureja informacijsko varnost. Če so zaradi zagotovitve višje ravni kibernetske varnosti, ob upoštevanju varnostnih tveganj, potrebni tudi sektorsko specifični ukrepi za operaterje, agencija lahko izda splošni akt, s katerim predpiše posebne tehnične usmeritve ter tehnične in organizacijske ukrepe, pri čemer upošteva tudi dokumente ali tehnična priporočila ENISA ter smernice Evropske komisije. Pri sprejemu splošnega akta agencija sodeluje z organom, pristojnim za informacijsko varnost.«.
- v prvem stavku četrtega odstavka 116. člena se besedilo »tretjega odstavka prejšnjega člena« nadomesti z besedilom »v skladu s prejšnjim členom«;
- 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 besedilo », razen določb 120. in 121. člena tega zakona, kjer nadzor izvaja organ, pristojen za informacijsko varnost.« nadomesti z besedilom »in izvajanje odločbe iz prvega odstavka 117. člena tega zakona.«;
- v prvem stavku prvega odstavka 287. člena se briše besedilo »ali organa, pristojnega za informacijsko varnost na podlagi 128. člena tega zakona«, besedilo iz tretjega stavka pa se nadomesti z besedilom »Agencija izvaja tudi nadzor nad izvajanjem odločbe vlade iz prvega odstavka 117. člena tega zakona.«;
- v 288. členu se za besedilom »po tem zakonu« doda besedilo »in po zakonu, ki ureja informacijsko varnost«;
- v 289. členu se črta tretji odstavek;
- v 298. členu se doda nova prva točka, ki se glasi »ne izvede odločbe vlade iz prvega odstavka 117. člena tega zakona,«, ostale točke se preštevilčijo;
- v 299. členu se črtajo 22., 23., 24., 26., 27., 28., 29. in 30. točka.

(3) Z dnem uveljavitve tega zakona prenehata veljati splošna akta izdana na podlagi sedmega odstavka 115. in iz drugega odstavka 118. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O), ki se smiselno uporabljata do pričetka uporabe podzakonskih aktov izdanih na podlagi tega zakona.

63. člen
(dopolnitev Zakona o prekrških)

V Zakonu o prekrških (Uradni list RS, št. 29/11 – uradno prečiščeno besedilo, 21/13, 111/13, 74/14 – odl. US, 92/14 – odl. US, 32/16, 15/17 – odl. US, 73/19 – odl. US, 175/20 – ZIUOPDVE in 5/21 – odl. US), se v petem odstavku 17. člena za besedilom »varstva konkurence« doda vejica in besedilo »informacijske varnosti«.

64. člen
(sprememba Zakona o varstvu osebnih podatkov)

V Zakonu o varstvu osebnih podatkov (Uradni list RS, št. 163/22) se v 4. točki prvega odstavka 23. člena besedilo »izvajalce bistvenih storitev« nadomesti z besedilom »pomembne subjekte«.

65. člen
(dokončanje postopkov, začetih pred uporabo tega zakona)

Upravni, inšpekcijski in prekrškovni postopki, ki do začetka uporabe tega zakona še niso bili pravnomočno končani, se končajo v skladu z dosedanjimi predpisi.

XII. Končna določba

66. člen
(začetek veljavnosti)

Ta zakon začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

- **PRILOGI I IN II K BESEDILU ČLENOV**

PRILOGA I

VISOKO KRITIČNI SEKTORJI

Sektor	Podsektor	Vrsta subjekta
1. Energija	(a) elektrika	—elektroenergetska podjetja, kot so opredeljena v členu 2, točka 57, Direktive (EU) 2019/944 Evropskega parlamenta in Sveta ([1]), ki opravljajo dejavnosti „dobave“, kot je opredeljena v členu 2, točka 12, navedene direktive
		—operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 29, Direktive (EU) 2019/944
		—operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 35, Direktive (EU) 2019/944
		—proizvajalci, kot so opredeljeni v členu 2, točka 38, Direktive (EU) 2019/944
		—imenovani operaterji trga električne energije, kot so opredeljeni v členu 2, točka 8, Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta ([2])
		—udeleženci na trgu, kot so opredeljeni v členu 2, točka 25, Uredbe (EU) 2019/943, ki opravljajo storitve agregiranja, prilagajanja odjema ali shranjevanja energije, kot so opredeljeni v členu 2, točke 18, 20 in 59, Direktive (EU) 2019/944
		—upravljavci polnilnega mesta, odgovorni za upravljanje in delovanje polnilnega mesta, ki končnim uporabnikom zagotavlja storitev polnjenja, tudi v imenu in za račun ponudnika mobilnostnih storitev
	(b)daljinsko ogrevanje in hlajenje	—upravljavci daljinskega ogrevanja ali daljinskega hlajenja, kot je opredeljeno v členu 2, točka 19, Direktive (EU) 2018/2001 Evropskega parlamenta in Sveta ([3])
	(c) nafta	— upravljavci naftovodov
		—upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in transporta nafte
		—osrednji organi za vzdrževanje zalog, kot so opredeljeni v členu 2, točka (f), Direktive Sveta 2009/119/ES ([4])
	(d) plin	—dobavitelji, kot so opredeljeni v členu 2, točka 8, Direktive 2009/73/ES Evropskega parlamenta in Sveta ([5])
		—operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 6, Direktive 2009/73/ES
		—operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 4, Direktive 2009/73/ES
		—operaterji skladiščnega sistema, kot so opredeljeni v členu 2, točka 10, Direktive 2009/73/ES

		—operaterji sistema za UZP, kot so opredeljeni v členu 2, točka 12, Direktive 2009/73/ES
		—podjetja plinskega gospodarstva, kot so opredeljeni v členu 2, točka 1, Direktive 2009/73/ES
		—upravljavci obratov za rafiniranje in predelavo zemeljskega plina
	(e) vodik	—upravljavci proizvodnje, shranjevanja in prenosa vodika
2. Promet	(a) zračni	—letalski prevozniki, kot so opredeljeni členu 3, točka 4, Uredbe (ES) št. 300/2008, ki se uporabljajo v komercialne namene
		—upravni organi letališča, kot so opredeljeni v členu 2, točka 2, Direktive 2009/12/ES Evropskega parlamenta in Sveta ([6]), letališča, kot so opredeljena v členu 2, točka 1, navedene direktive, vključno z jedrnimi letališči iz oddelka 2 Priloge II k Uredbi (EU) št. 1315/2013 Evropskega parlamenta in Sveta ([7]), ter subjekti, ki upravljajo pomožne objekte, naprave in sredstva na letališčih
		—kontrolorji upravljanja prometa, ki zagotavljajo kontrolo zračnega prometa (ATC), kot je opredeljena v členu 2, točka 1, Uredbe (ES) št. 549/2004 Evropskega parlamenta in Sveta ([8])
	(b) železniški	—upravljavci infrastrukture, kot so opredeljeni v členu 3, točka 2, Direktive 2012/34/EU Evropskega parlamenta in Sveta ([9])
		—prevozniki v železniškem prometu, kot so opredeljeni v členu 3, točka 1, Direktive 2012/34/EU, vključno z upravljavci objektov za izvajanje železniških storitev, kot so opredeljeni v členu 3, točka 12, navedene direktive
	(c) vodni	—prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, kot so za področje vodnega prometa opredeljena v Prilogi I k Uredbi (ES) št. 725/2004 Evropskega parlamenta in Sveta ([10]), brez posameznih plovil, ki jih upravljajo ta podjetja
		—upravni organi pristanišč, kot so opredeljena v členu 3, točka 1, Direktive 2005/65/ES Evropskega parlamenta in Sveta ([11]), vključno z njihovimi pristanišči, kot so opredeljena v členu 2, točka 11, Uredbe (ES) št. 725/2004, ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih
		—upravljavci sistemov za nadzor plovbe (VTS), kot so opredeljeni v členu 3, točka (o), Direktive 2002/59/ES Evropskega parlamenta in Sveta ([12])
	(d) cestni	—cestni organi, kot so opredeljeni v členu 2, točka 12, Delegirane uredbe Komisije (EU) 2015/962 ([13]), odgovorni za nadzor upravljanja prometa, razen javnih subjektov, za katere je upravljanje prometa ali upravljanje inteligentnih prometnih sistemov le nebistven del splošne

		dejavnosti
		—upravljavci inteligentnih prometnih sistemov, kot so opredeljeni v členu 4, točka 1, Direktive 2010/40/EU Evropskega parlamenta in Sveta [14]
3. Bančništvo		kreditne institucije, kot so opredeljene v členu 4, točka 1, Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta [15]
4.Infrastruktura finančnega trga		—upravljavci mest trgovanja, kot so opredeljena v členu 4, točka 24, Direktive 2014/65/EU Evropskega parlamenta in Sveta [16]
		—centralne nasprotne stranke (CNS), kot so opredeljene v členu 2, točka 1, Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta [17]
5. Zdravje		—izvajalci zdravstvenega varstva, kot so opredeljeni v členu 3, točka (g), Direktive 2011/24/EU Evropskega parlamenta in Sveta [18]
		—referenčni laboratoriji EU iz člena 15 Uredbe (EU) 2022/2371 Evropskega parlamenta in Sveta [19]
		—subjekti, ki izvajajo raziskovalne in razvojne dejavnosti na področju zdravil, kot so opredeljena v členu 1, točka 2, Direktive 2001/83/ES Evropskega parlamenta in Sveta [20] —subjekti, ki proizvajajo farmacevtske surovine in preparate s področja C oddelka 21 NACE Rev. 2 —subjekti, ki proizvajajo medicinske pripomočke, ki se štejejo za kritične v času izrednih razmer v javnem zdravju (seznam kritičnih pripomočkov v izrednih razmerah v javnem zdravju) v smislu člena 22 Uredbe (EU) 2022/123 Evropskega parlamenta in Sveta [21]
6. Pitna voda		dobavitelji in distributerji vode, namenjene za prehrano ljudi, kot je opredeljena v členu 2, točka 1(a), Direktive (EU) 2020/2184 Evropskega parlamenta in Sveta [22], razen distributerjev, za katere je distribucija vode za prehrano ljudi le nebistven del splošne dejavnosti distribucije drugih dobrin in blaga
7.Odpadna voda		podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo, odpadno vodo iz gospodinjstev ali tehnološko odpadno vodo, kot je opredeljena v členu 2, točke 1, 2 in 3, Direktive Sveta 91/271/EGS [23], razen podjetij, za katera je zbiranje, odvajanje ali čiščenje komunalne odpadne vode, odpadne vode iz gospodinjstev ali tehnološke odpadne vode nebistven del splošne dejavnosti
8.Digitalna infrastruktura		— ponudniki stičišča omrežij
		—ponudniki storitev DNS, razen upravljavcev korenskih imenskih strežnikov
		— registri TLD imen
		— ponudniki storitev računalništva v oblaku

		— ponudniki storitev podatkovnih centrov
		— ponudniki omrežij za dostavo vsebin
		— ponudniki storitev zaupanja
		—ponudniki javnih elektronskih komunikacijskih omrežij
		—ponudniki javno dostopnih elektronskih komunikacijskih storitev
9.Upravljanje storitev IKT		— ponudniki upravljanih storitev — ponudniki upravljanih varnostnih storitev
10.Javna uprava		—subjekti javne uprave enot centralne ravni držav, kot jih opredeli država članica v skladu z nacionalnim pravom
		—subjekti javne uprave enot na regionalni ravni, kot jih opredeli država članica v skladu z nacionalnim pravom
11. Vesolje		upravljavci talne infrastrukture, ki jo imajo v lasti, vodijo in upravljajo države članice ali zasebne stranke, ki podpirajo opravljanje vesoljskih storitev, brez ponudnikov javnih elektronskih komunikacijskih omrežij

(1) Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14.6.2019, str. 125).

(2) Uredba (EU) 2019/943 Evropskega parlamenta in Sveta z dne 5. junija 2019 o notranjem trgu električne energije (UL L 158, 14.6.2019, str. 54).

(3) Direktiva (EU) 2018/2001 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o spodbujanju uporabe energije iz obnovljivih virov (UL L 328, 21.12.2018, str. 82).

(4) Direktiva Sveta 2009/119/ES z dne 14. septembra 2009 o obveznosti držav članic glede vzdrževanja minimalnih zalog surove nafte in/ali naftnih derivatov (UL L 265, 9.10.2009, str. 9).

(5) Direktiva 2009/73/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o skupnih pravilih notranjega trga z zemeljskim plinom in o razveljavitvi Direktive 2003/55/ES (UL L 211, 14.8.2009, str. 94).

(6) Direktiva 2009/12/ES Evropskega parlamenta in Sveta z dne 11. marca 2009 o letaliških pristojbinah (UL L 70, 14.3.2009, str. 11).

(7) Uredba (EU) št. 1315/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o smernicah Unije za razvoj vseevropskega prometnega omrežja in razveljavitvi Sklepa št. 661/2010/EU (UL L 348, 20.12.2013, str. 1).

(8) Uredba (ES) št. 549/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o določitvi okvira za oblikovanje enotnega evropskega neba (okvirna uredba) (UL L 96, 31.3.2004, str. 1).

(9) Direktiva 2012/34/EU Evropskega parlamenta in Sveta z dne 21. novembra 2012 o vzpostavitvi enotnega evropskega železniškega območja (UL L 343, 14.12.2012, str. 32).

(10) Uredba (ES) št. 725/2004 Evropskega parlamenta in Sveta z dne 31. marca 2004 o povečanju zaščite na ladjah in v pristaniščih (UL L 129, 29.4.2004, str. 6).

(11) Direktiva Evropskega parlamenta in Sveta 2005/65/ES z dne 26. oktobra 2005 o krepitvi varnosti v pristaniščih (UL L 310, 25.11.2005, str. 28).

(12) Direktiva 2002/59/ES Evropskega parlamenta in Sveta z dne 27. junija 2002 o vzpostavitvi sistema spremljanja in obveščanja za ladijski promet ter o razveljavitvi Direktive Sveta 93/75/EGS (UL L 208, 5.8.2002, str. 10).

(13) Delegirana uredba Komisije (EU) 2015/962 z dne 18. decembra 2014 o dopolnitvi Direktive 2010/40/EU Evropskega parlamenta in Sveta v zvezi z opravljanjem storitev zagotavljanja prometnih informacij v realnem času po vsej EU (UL L 157, 23.6.2015, str. 21).

(14) Direktiva 2010/40/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza (UL L 207, 6.8.2010, str. 1).

(15) Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

(16) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349).

(17) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).

(18) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4.4.2011, str. 45).

([19]) Uredba (EU) 2022/2371 Evropskega parlamenta in Sveta z dne 23. novembra 2022 o resnih čezmejnih grožnjah za zdravje in o razveljavitvi Sklepa št. 1082/2013/EU (UL L 314, 6.12.2022, str. 26).

([20]) Direktiva 2001/83/ES Evropskega parlamenta in Sveta z dne 6. novembra 2001 o zakoniku Skupnosti o zdravilih za uporabo v humani medicini (UL L 311, 28.11.2001, str. 67).

([21]) Uredba (EU) 2022/123 Evropskega parlamenta in Sveta z dne 25. januarja 2022 o okrepljeni vlogi Evropske agencije za zdravila pri pripravljenosti na krize in kriznem upravljanju na področju zdravil in medicinskih pripomočkov (UL L 20, 31.1.2022, str. 1).

([22]) Direktiva (EU) 2020/2184 Evropskega parlamenta in Sveta z dne 16. decembra 2020 o kakovosti vode, namenjene za prehrano ljudi (UL L 435, 23.12.2020, str. 1).

([23]) Direktiva Sveta 91/271/EGS z dne 21. maja 1991 o čiščenju komunalne odpadne vode (UL L 135, 30.5.1991, str. 40).

PRILOGA II

DRUGI KRITIČNI SEKTORJI

Sektor	Podsektor	Vrsta subjekta
1. Poštne in kurirske storitve		izvajalci poštnih storitev, kot so opredeljeni v členu 2, točka 1a, Direktive 97/67/ES, vključno z izvajalci kurirskih storitev
2. Ravnanje z odpadki		podjetja, ki izvajajo postopke ravnanja z odpadki, kot je opredeljeno v členu 3, točka 9, Direktive 2008/98/ES Evropskega parlamenta in Sveta ([1]), vendar brez podjetij, pri katerih ravnanje z odpadki ni glavna gospodarska dejavnost
3. Izdelava, proizvodnja in distribucija kemikalij		podjetja, ki proizvajajo snovi in distribuirajo snovi ali zmesi iz člena 3, točki 9 in 14, Uredbe (ES) št. 1907/2006 Evropskega parlamenta in Sveta ([2]) in podjetja, ki iz snovi in zmesi proizvajajo izdelke, kot so opredeljeni v členu 3, točka 3, navedene uredbe
4. Pridelava, predelava in distribucija živil		živilske dejavnosti, kot so opredeljene v členu 3, točka 2, Uredbe (ES) št. 178/2002 Evropskega parlamenta in Sveta ([3]), ki se ukvarjajo s prodajo na debelo ter industrijsko pridelavo in predelavo
5. Proizvodnja	(a) proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov	subjekti, ki proizvajajo medicinske pripomočke, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) 2017/745 Evropskega parlamenta in Sveta ([4]), in subjekti, ki proizvajajo in vitro diagnostične medicinske pripomočke, kot so opredeljeni v členu 2, točka 2, Uredbe (EU) 2017/746 Evropskega parlamenta in Sveta ([5]), razen subjektov, ki proizvajajo medicinske pripomočke iz Priloge I, točka 5, peta alinea, k tej direktivi
	(b) proizvodnja računalnikov, elektronskih in optičnih izdelkov	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 26 NACE Rev. 2
	(c) proizvodnja električnih naprav	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 27 NACE Rev. 2
	(d) proizvodnja drugih strojev in naprav	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 28 NACE Rev. 2
	(e) proizvodnja	podjetja, ki opravljajo katero koli gospodarsko

	motornih vozil, prikolic in polprikolic	dejavnost s področja C oddelka 29 NACE Rev. 2
	(f)proizvodnja drugih vozil in plovil	podjetja, ki opravljajo katero koli gospodarsko dejavnost s področja C oddelka 30 NACE Rev. 2
6.Digitalni ponudniki		— ponudniki spletnih tržnic
		— ponudniki spletnih iskalnikov
		—ponudniki platform za storitve družbenega mreženja
7. Raziskave		raziskovalne organizacije

[1] Direktiva 2008/98/ES Evropskega parlamenta in Sveta z dne 19. novembra 2008 o odpadkih in razveljavitvi nekaterih direktiv (UL L 312, 22.11.2008, str. 3).

[2] Uredba (ES) št. 1907/2006 Evropskega parlamenta in Sveta z dne 18. decembra 2006 o registraciji, evalvaciji, avtorizaciji in omejevanju kemikalij (REACH) ter o ustanovitvi Evropske agencije za kemikalije in o spremembi Direktive 1999/45/ES ter o razveljavitvi Uredbe Sveta (EGS) št. 793/93 in Uredbe Komisije (ES) št. 1488/94 ter Direktive Sveta 76/769/EGS in direktiv Komisije 91/155/EGS, 93/67/EGS, 93/105/ES in 2000/21/ES (UL L 396, 30.12.2006, str. 1).

[3] Uredba (ES) št. 178/2002 Evropskega parlamenta in Sveta z dne 28. januarja 2002 o določitvi splošnih načel in zahtevah živilske zakonodaje, ustanovitvi Evropske agencije za varnost hrane in postopkih, ki zadevajo varnost hrane (UL L 31, 1.2.2002, str. 1).

[4] Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1).

[5] Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o *in vitro* diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

III. OBRAZLOŽITEV

PREDSTAVITEV ČLENOV

I. Splošne določbe

V poglavju o splošnih določbah predlog zakona določa vsebino zakona, njegov namen in področje uporabe, vsebuje določbe glede obdelave podatkov in informacij ter opredeljuje pomen izrazov.

K 1. členu

Predlog člena opredeljuje vsebino zakona, ki predstavlja sistemsko osnovo za celovito ureditev informacijske in kibernetske varnosti na določenih ključnih področjih v Republiki Sloveniji.

Predlog zakona tako 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.

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 in prostovoljno priglasitev incidentov. Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu vključno za področje certificiranja kibernetske varnosti.

Predlagana določba pri tem vključuje tudi vsebine iz 1. člena (Predmet urejanja) 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. 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) š. 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 (EU) 2022/2555).

K 2. členu

Predlog člena v prvem odstavku pojasnjuje namen predloga zakona, ki je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti vključno s krepitvijo zaupanja v proizvode IKT, storitve IKT in postopke IKT ter njihove varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah.

Drugi odstavek člena določa, da se s tem zakonom v pravni red Republike Slovenije prenaša Direktiva (EU) 2022/2555.

Tretji odstavek člena pa določa, zakon ureja izvajanje 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) (UL L št. 151 z dne 7. 6. 2019, str. 15; v nadaljnjem besedilu: Uredba (EU) 2019/881). Ob tem pojasnjujemo, da je že Zakon o spremembah in dopolnitvi Zakona o informacijski varnosti (Uradni list RS, št. 95/21; v nadaljnjem besedilu: ZInfV-A), ki je s 5. členom posegel v 27. člen dotedanjega zakona, v luči Uredbe (EU) 2019/881 pristojnemu nacionalnemu organov v drugem odstavku prej navedenega člena pristojnemu nacionalnemu organu dodal tudi nalogo pod točko 18. "izvaja naloge nacionalnega certifikacijskega organa". Ugotavljamo, da je za izvajanje sicer neposredno uporabljive Uredbe (EU) 2019/8881 treba dodatno urediti še nekatere dodatne vsebine, kar se udejanja s predlaganim zakonom.

Ob tem je treba pojasniti, da predlagani zakon ob upoštevanju njegovega namena iz prvega odstavka predlaganega člena poleg prenosa Direktive (EU) 2022/2555 sistemsko ureja področje informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji tudi na področjih, ki niso zajeta z Direktivo (EU) 2022/2555 (ki je direktiva notranjega trga ter direktiva minimalne harmonizacije), so pa bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah. V tem smislu predlagani zakon sledi sistemskemu načinu urejanja iz Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV), ki ga nadomešča. Predlagani zakon vsebuje torej tudi nacionalne določbe, ki so potrebne za zagotovitev namena predstavljenega v prvem odstavku tega člena.

K 3. členu

S predlogom tega člena se določa področje uporabe predlaganega zakona. Pri tem predlagani člen v pretežni meri sledi 2. členu (Področje uporabe) Direktive (EU) 2022/2555, vendar ob upoštevanju nacionalnih pristojnosti urejanja na področjih, ki niso bila pogodbeno prenesena na Evropsko Unijo (v nadaljnjem besedilu: Unija) in jih predmetna direktiva (ki je direktiva notranjega trga) zato izključuje iz področja svoje uporabe. Posledično predlagani zakon ne izključuje v celoti njegove uporabe za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, kot to izhaja iz sedmega odstavka Direktive (EU) 2022/2555, upošteva pa se šesti odstavek Direktive (EU) 2022/2555, po katerem ta direktiva ne posega v pristojnosti držav članic, da zaščitijo nacionalno varnost, in v njihova pooblastila za zaščito drugih bistvenih državnih funkcij, vključno z zagotavljanjem ozemeljske celovitosti države ter vzdrževanjem javnega reda in miru. Pri tem uvodna izjava 13 prej navedene direktive pojasnjuje: »Glede na okrepitev in večjo izpopolnjenost kibernetskih groženj bi si morale države članice prizadevati zagotoviti, da subjekti, ki so izključeni s področja uporabe te direktive, dosežejo visoko raven kibernetske varnosti, in podpirati izvajanje enakovrednih ukrepov za obvladovanje tveganj za kibernetsko varnost, ki odražajo občutljivo naravo teh subjektov.«. Upoštevajo se tudi določbe 5. člena Direktive (EU) 2022/2555 (Minimalna harmonizacija), po kateri ta direktiva državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetske varnosti, pod pogojem, da so take določbe v skladu z obveznostmi držav članic, določenimi v pravu Unije.

Ob tem pa že Direktiva (EU) 2022/2555 v uvodni izjavi šest pojasni, da bi bilo z razveljavitvijo Direktive (EU) 2016/1148[1], treba področje uporabe po sektorjih razširiti na večji del gospodarstva, da bi se zagotovila celovita pokritost sektorjev in storitev, ki so bistvenega pomena za ključne družbene in gospodarske dejavnosti na notranjem trgu. Ta širitev področja uporabe po sektorjih je razvidna iz Priloge I (Visoko kritični sektorji) in Priloge II (Drugi kritični sektorji) Direktive (EU) 2022/2555, ki naštevata sektorje, v določenih primerih pa tudi podsektorje, znotraj katerih delujejo v obeh prilogah naštete vrste subjektov, kar je relevantno z vidika področja uporabe te direktive. Pri tem Direktiva (EU) 2022/2555, kot osnovno pravilo (od katerega v nekaterih primerih odstopa) postavlja pravilo velikosti.

[1] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

Glede prej navedenega uvodna izjava sedem Direktive (EU) 2022/2555 pojasnjuje: »Na podlagi Direktive (EU) 2016/1148 so bile države članice odgovorne za določitev subjektov, ki izpolnjujejo merila, na podlagi katerih se štejejo za izvajalce bistvenih storitev. Za odpravo velikih razlik med državami članicami v zvezi s tem in zagotovitev pravne varnosti v zvezi z ukrepi kibernetske varnosti za obvladovanje tveganja in obveznosti poročanja za vse ustrezne subjekte bi bilo treba določiti enotno merilo, ki bi določalo, kateri subjekti spadajo na področje uporabe te direktive. To merilo bi moralo vključevati uporabo pravila omejitve velikosti, v skladu s katerim na področje uporabe te direktive spadajo vsi subjekti, ki se na podlagi člena 2 Priloge k Priporočilu Komisije 2003/361/ES[2] štejejo za srednja podjetja, ali presegajo zgornje meje za srednja podjetja iz odstavka 1 navedenega člena, in ki delujejo v sektorjih in opravljajo vrste storitev ali izvajajo dejavnosti, zajete s to direktivo. Države članice bi morale tudi zagotoviti, da na področje uporabe te direktive spadajo nekatera mala podjetja in mikro podjetja, kot so opredeljena v členu 2(2) in (3) navedene priloge, ki izpolnjujejo posebna merila, ki kažejo na ključno vlogo za družbo, gospodarstvo ali za določene sektorje ali vrste storitev.«.

Določba prvega odstavka 2. člena Direktive (EU) 2022/2555 kot splošno pravilo njenega področja uporabe zato določa, da se ta direktiva uporablja za javne ali zasebne subjekte vrste iz Priloge I ali II navedene direktive, ki izpolnjujejo pogoje za srednja podjetja iz člena 2 Priloge Priporočilu 2003/361/ES, ali presegajo zgornje meje za srednja podjetja, določene v odstavku 1 navedenega člena, in ki opravljajo svoje storitve ali izvajajo svoje dejavnosti v Uniji. Člen 3(4) Priloge k navedenemu priporočilu pa se ne uporablja za namene te direktive. Navedeno splošno pravilo področja uporabe se prenaša v predlagani zakon s prvim odstavkom predlaganega člena, po katerem se ta zakon uporablja za javne ali zasebne subjekte vrste iz Prilog predlaganega zakona I ali II (v nadaljnjem besedilu Priloga I ali II), ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov, kar ustreza kriterijem te direktive in priporočila, na katerega se sklicuje. Drugi odstavek predlaganega člena določa primere, kot se predlagani zakon uporablja za subjekte iz prejšnjega odstavka (gre torej za subjekte vrste iz Priloge I ali II) ne glede na njihovo velikost ali letni promet oziroma letno bilančno vsoto in sicer, kadar: 1. opravljajo storitev ponudnika javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ponudniki storitev zaupanja ali registra 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; 6. gre za subjekt javne uprave na državni ravni ali na regionalni oziroma lokalni ravni, če pri slednjem izhaja iz ocene tveganja, da opravljajo storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti. Ta predlagana določba pomeni prenos drugega odstavka 2. člena Direktive (EU) 2022/2555. Z vidika možnosti nacionalne širitve se pri točkah 5 in 6 dodaja še lokalna raven, namreč po točki (a) petega odstavka 2. člena Direktive (EU) 2022/2555, države članice lahko določijo, da se ta direktiva uporablja tudi za subjekte javne uprave na lokalni ravni. Republika Slovenija trenutno (še) nima regionalne ravni lokalne samouprave, se jo pa vključuje v predlagani zakon skladno z Direktivo (EU) 2022/2555. V primeru vzpostavitve regionalne samouprave tako ne bo treba zgolj iz tega razloga dopolnjevati sedaj predlagane zakonske ureditve. Prav tako se z vidika možnosti nacionalne širitve na tem mestu dodaja še točka 7 in sicer, kadar 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.

[2] Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

Tretji odstavek predlaganega člena določa, da se ta zakon uporablja tudi za subjekte, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo, torej gre za vse subjekte, ki so tako določeni, ne glede na njihovo velikost. Pri tem gre za prenos tretjega odstavka 2. člena Direktive (EU) 2022/2555, ki določa, da se ta direktiva uporablja tudi za subjekte, ki so identificirani kot kritični na podlagi Direktive (EU) 2022/2557[3], ne glede na njihovo velikost, pri čemer se ta direktiva istočasno prenaša v slovenski pravni red z (novim) zakonom, ki ureja kritično infrastrukturo.

Četrti odstavek predlaganega člena določa, da se ta zakon uporablja tudi za subjekte, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost, kar je prenos četrtega odstavka 2. člena Direktive (EU) 2022/2555.

Peti odstavek predlaganega člena je nacionalna določba, ki upoštevaje 5. člen Direktive (EU) 2022/2555 (minimalna harmonizacija) širi področje uporabe tega zakona še na organe, ki v skladu z državnimi načrti zaščite in reševanja izvajajo naloge na področju zaščite in reševanja, v kolikor takšni organi niso že zajeti med subjekti, za katere se uporablja ta zakon, na podlagi prejšnjih odstavkov tega člena. Državni načrti zaščite in reševanja, ki jih pripravi Uprava Republike Slovenije za zaščito in reševanje v sodelovanju z ministrstvi in drugimi državnimi organi ter ustreznimi strokovnimi organizacijami, namreč med organi, ki izvajajo naloge v skladu s temi načrti lahko vsebujejo tudi organe, ki sicer ne bili vključeni med subjekte, ki sicer spadajo v področje uporabe tega zakona. Ocenjujemo namreč, da je pri vseh organih, ki izvajajo naloge v skladu z državnimi načrti zaščite in reševanja pomembno, da njihovi omrežni in informacijski sistemi delujejo oziroma so čimbolj odporni na kibernetske incidente in grožnje, saj bi nedelovanje njihovih sistemov ob večji nesreči ali krizi, lahko vplivalo tudi na reševanje človeških življenj in premoženja večje vrednosti.

Šesti odstavek predlaganega člena določa uporabo tega zakona tudi za subjekte lokalne samouprave in sicer za mestne občine in občine, ki imajo sedeže v krajih, kjer so sedeži upravnih enot, pri čemer se upošteva točka (a) petega odstavka 2. člena Direktive (EU) 2022/2555, po kateri države članice lahko določijo, da se ta direktiva uporablja tudi za subjekte javne uprave na lokalni ravni.

Sedmi odstavek tega člena določa, da se zakon ne uporablja za subjekte, ki jih je Republika Slovenija izvzela s področja uporabe Uredbe (EU) 2022/2554 v skladu s četrtim odstavkom 2. člena prej navedene uredbe. Navedeno ustreza desetemu odstavku 2. člena Direktive (EU) 2022/2555, po katerem se ta direktiva ne uporablja za subjekte, ki so jih države članice izvzele s področja uporabe Uredbe (EU) 2022/2554[4] v skladu s členom 2(4) navedene uredbe.

Po osmem odstavku predlaganega člena ta zakon ne posega v izvajanje predpisov s področja varstva osebnih podatkov (gre za Zakon o varstvu osebnih podatkov - ZVOP-2 in za Splošno uredbo o varstvu podatkov Evropske unije) in zasebnosti na področju elektronskih komunikacij (gre za Zakon o elektronskih komunikacijah – ZEKom-2) , s področja boja proti spolni zlorabi otrok in proti izdelavi, razširjanju in hrambi gradiva, ki prikazuje spolno zlorabo otrok, predpisa o napadih na informacijske sisteme (v obeh primerih gre za Kazenski zakonik – KZ-1 - navedeno ustreza dvanajstemu odstavka 2. člena Direktive (EU) 2022/2555, po katerem se ta direktiva med drugim uporablja brez poseganja v direktivi 2011/93/EU[5] in 2013/40/EU[6]), n s področja kritične infrastrukture (gre za Zakon o kritični infrastrukturi – ZKI).

Pri devetem, desetem in enajstem odstavku predlaganega člena gre za prenos člena 4 (Sektorski pravni akti Unije) Direktive (EU) 2022/2555, ki v prvem odstavku določa pravila in pogoje za izključitev iz uporabe zadevnih določb te direktive za bistvene ali pomemben subjekte, ki bi sicer spadali v njeno področje uporabe, pa sektorski pravni akti Unije za njih vsebujejo po učinku vsaj enakovredne zahteve

[3] Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljaviti Direktive Sveta 2008/114/ES (UL L št. 333/142, z dne 27. 12. 2022, str. 164).
[4] Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L št. 333/142, z dne 27. 12. 2022, str. 1).
[5] Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL L 335, 17.12.2011, str. 1).
[6] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).

bodisi za obvladovanje tveganj za kibernetsko varnost bodisi za priglasitev incidentov. Pri tem je v drugem odstavku 4. člena določeno tudi, kdaj se takšne zahteve štejejo za enakovredne zahtevam te direktive, v tretjem odstavku pa so bile napovedane tudi Smernice Evropske komisije o uporabi prvega in drugega odstavka tega člena, ki so bile medem že sprejete[7]. Že uvodni izjavi 28 in 29 Direktive (EU) 2022/2555 pa glede takšne po učinku enakovredne sektorske zakonodaje podajata primera, ki se nanašata na finančni sektor ter na letalski sektor in se glasita:

»(28) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta (10) bi se morala šteti za sektorski pravni akt Unije v zvezi s to direktivo, kar zadeva finančne subjekte. Določbe Uredbe (EU) 2022/2554 v zvezi z ukrepi za obvladovanje tveganj na področju informacijske in komunikacijske tehnologije (IKT), obvladovanjem incidentov, povezanih z IKT, in zlasti poročanjem o večjih incidentih, povezanih z IKT, kot tudi testiranjem digitalne operativne odpornosti, dogovori o izmenjavi informacij in tveganjem tretjih oseb na področju IKT bi se morale uporabljati namesto določb te direktive. Države članice zato ne bi smele uporabljati določb te direktive o obvladovanju tveganj za kibernetsko varnost in obveznostih poročanja ter nadzoru in izvrševanju za finančne subjekte, zajete z Uredbo (EU) 2022/2554. Hkrati je pomembno ohranjati tesno povezavo in izmenjavo informacij s finančnim sektorjem na podlagi te direktive. V ta namen Uredba (EU) 2022/2554 evropskim nadzornim organom in pristojnim organom iz navedene uredbe omogoča, da sodelujejo pri dejavnostih skupine za sodelovanje ter si izmenjujejo informacije in sodelujejo z enotnimi kontaktnimi točkami, kot tudi s skupinami CSIRT in pristojnimi organi iz te direktive. Pristojni organi iz Uredbe (EU) 2022/2554 bi morali podrobnosti o večjih incidentih, povezanih z IKT, in po potrebi pomembnih kibernetskih grožnjah posredovati tudi skupinam CSIRT, pristojnim organom ali enotnim kontaktnim točkam iz te direktive. To je mogoče doseči z zagotovitvijo takojšnjega dostopa do priglasitev incidentov in njihovega posredovanja neposredno ali prek enotne vstopne točke. Poleg tega bi morale države članice še naprej vključevati finančni sektor v svoje strategije za kibernetsko varnost, skupine CSIRT pa lahko vključijo finančni sektor v svoje dejavnosti.

(29) V izogib vrzelim ali podvajanju obveznosti glede kibernetske varnosti, ki veljajo za subjekte v letalskem sektorju, bi morali nacionalni organi iz uredb (ES) št. 300/2008 (11) in (EU) 2018/1139 (12) Evropskega parlamenta in Sveta ter pristojni organi iz te direktive sodelovati pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost in nadzoru spoštovanja teh ukrepov na nacionalni ravni. Pristojni organi iz te direktive bi lahko skladnost subjekta z varnostnimi zahtevami iz uredb (ES) št. 300/2008 in (EU) 2018/1139 ter iz ustreznih delegiranih in izvedbenih aktov, sprejetih na podlagi navedenih uredb, šteli za skladnost z ustreznimi zahtevami iz te direktive.«

V enajstem odstavku se poleg zgoraj navedenega zaradi lažje uporabe zakona s strani njegovih uporabnikov in zavezancev ter večje preglednosti, določa tudi dodatna (nacionalna) obveznost pristojnega nacionalnega organa, da vodi ažuren seznam neposredno uporabljivih EU predpisov in nacionalnih predpisov, ki so po učinku enakovredni določbam tega zakona. Predlog za uvrstitev na takšne seznam, ki mora biti v skladu z devetim in prejšnjim odstavkom tega člena ter ob upoštevanju smernic iz tega odstavka, pa pristojnemu nacionalnemu organu posreduje za posamični predpis pristojno resorno ministrstvo ali regulatorni organ, če je pooblaščen za sprejem ustreznega akta. Ta predlog upošteva, da imajo najboljši pregled nad posamezno področno zakonodajo resorno pristojna ministrstva oziroma regulatorni organi iz posamičnega področja urejanja oziroma reguliranja. Po prejemu predloga za uvrstitev na tak seznam pa je pristojni nacionalni organ tisti, ki po presoji izpolnjevanja pogojev uvrsti posamični EU ali nacionalni predpis na seznam takšnih predpisov, ki se objavi na spletni strani pristojnega nacionalnega organa. Takšna predlagana ureditev izhaja iz dejstva, da se enakovrednost učinkov ukrepov za obvladovanje tveganj za kibernetsko varnost in zahtev glede prijave incidentov ter možnost samodejnega in enakovrednega dostopa do priglasitev incidentov presoja glede na ureditev predlaganega horizontalnega zakona, ki pa spada v pristojnost pristojnega nacionalnega organa.

[7] Gre za Sporočilo Komisije - Smernice Komisije o uporabi člena 4 (1) in (2) Direktive (EU) 2022/2555 (Direktiva NIS) (UL C 328, z dne 18. 9. 2023, str. 2)

Dvanajsti odstavek upošteva, da se glede na namen predlaganega zakona iz njegovega tretjega odstavka 2. člena z njim dodatno ureja tudi izvajanje Uredbe (EU) 2019/881. Fizične in pravne osebe, ki jih naslavlja neposredno uporabljiva Uredba (EU) 2019/881, niso v celoti zajeti med subjekti, ki sicer spadajo v področje uporabe predlaganega zakona na podlagi prejšnjih odstavkov tega člena. Zato je bilo v predlaganem zakonu treba posebej opredeliti tudi, da se ta zakon (zgolj) v delu, ki se nanaša na področje certificiranja kibernetske varnosti, uporablja tudi za druge fizične in pravne osebe, ki niso bistveni ali pomembni subjekti po tem zakonu, ki jih zadeva Uredba (EU) 2019/881 v delu, ki ureja certifikacijski okvir za kibernetsko varnost.

K 4. členu

Določba štirinajstega odstavka 2. člena Direktive (EU) 2022/2555, določa, da subjekti, pristojni organi, enotne kontaktne točke in skupine CSIRT obdelujejo osebne podatke v obsegu, ki je potreben za namene te direktive, in v skladu z Uredbo (EU) 2016/679 (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov)[8], pri čemer mora taka obdelava zlasti temeljiti na členu 6 Uredbe. Kar zadeva obdelavo osebnih podatkov na podlagi te direktive (torej Direktive (EU) 2022/2555), jo morajo ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev izvajati v skladu s pravom Unije o varstvu podatkov in pravom Unije o zasebnosti, zlasti z Direktivo 2002/58/ES (v nadaljnjem besedilu: Direktiva o zasebnosti in elektronskih komunikacijah)[9]. Uvodna izjava 14 Direktive (EU) 2022/2555 se pri tem glasi: »Pravo Unije o varstvu podatkov in pravo Unije o zasebnosti se uporablja za vsakršno obdelavo osebnih podatkov na podlagi te direktive. Ta direktiva zlasti ne posega v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ter Direktivo 2002/58/ES Evropskega parlamenta in Sveta. Ta direktiva zato med drugim ne bi smela vplivati na naloge in pooblastila organov, pristojnih za spremljanje skladnosti z veljavnim pravom Unije o varstvu podatkov in pravom Unije o zasebnosti.«.

Zato prvi odstavek predlaganega člena najprej določa, da se obdelava osebnih podatkov na podlagi tega zakona izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev pa jo izvajajo tudi v skladu s predpisom, ki ureja zasebnost na področju elektronskih komunikacij. Pri tem pojasnjujmo, da Direktivo o zasebnosti in elektronskih komunikacijah v slovenski pravni red prenaša zakon, ki ureja elektronske komunikacije, trenutno je to Zakon o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2) v svojem XII. poglavju, ki ima naslov »OBEDELAVA OSEBNIH PODATKOV IN VARSTNO ZASEBNOSTI ELEKTRONSKIH KOMUNIKACIJ«. Pri tem že prvi člen tega poglavja (to je 211. člen ZEKom-2) v tretjem odstavku pojasni, da to poglavje ureja obdelavo osebnih podatkov v zvezi z zagotavljanjem javnih komunikacijskih storitev v javnih komunikacijskih omrežjih, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave. Med predpise s področja varstva osebnih podatkov poleg Splošne uredbe o varstvu podatkov v slovenskem pravnem redu spada predvsem Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22: v nadaljnjem besedilu: ZVOP-2). Nadalje se v predlagani določbi prvega odstavka tega člena zaradi jasnosti še določa, da obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij pomeni zakoniti interes zadevnega upravljavca podatkov. Pri tem smo izhajali iz uvodne izjave 49 Splošne uredbe o varstvu podatkov, ki pojasnjuje: »Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežja in informacij, tj. zmožnosti omrežja ali informacijskega sistema, da na določeni ravni zaupanja prepreči slučajne dogodke ali nezakonita ali zlonamerna dejanja, ki ogrožajo dostopnost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih osebnih podatkov ter varnost s tem povezanih

[8] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).
[9] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

storitev, ki jih ponujajo ali so dostopne prek teh omrežij in sistemov, s strani javnih organov, skupin za odzivanje na računalniške grožnje, skupin za odzivanje na računalniške varnostne incidente, ponudnikov elektronskih komunikacijskih omrežij in storitev ter ponudnikov varnostnih tehnologij in storitev pomeni zakoniti interes zadevnega upravljavca podatkov. To bi lahko vključevalo na primer preprečevanje nepooblaščenega dostopa do elektronskih komunikacijskih omrežij, širjenja zlonamernih kod, napadov, ki povzročajo zavrnitev storitve, ter škode na računalniških in elektronskih komunikacijskih sistemih.«.

V nadaljevanju predlagani člen ob upoštevanju nacionalnih posebnosti v predlagani zakon prenaša trinajsti odstavek 2. člena Direktive (EU) 2022/2555, ki določa: »Brez poseganja v člen 346 PDEU se informacije, ki so zaupne v skladu s predpisi Unije ali nacionalnimi predpisi, na primer o poslovni tajnosti, s Komisijo in drugimi ustreznimi organi v skladu s to direktivo izmenjajo le, kadar je takšna izmenjava potrebna za uporabo te direktive. Izmenjava informacij se omeji na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave. Pri izmenjavi informacij se ohrani zaupnost zadevnih informacij ter zaščitijo varnost in poslovni interesi zadevnih subjektov.«. Posledično je v drugem odstavku predlaganega člena z vidika varstva zaupnosti podatkov in informacij, ki se obdelujejo na podlagi predlaganega zakona in so opredeljeni kot tajni ali kot poslovna skrivnost ali druge oblike varovanih podatkov, predlagano, da se le-ti obravnavajo v skladu s področnimi predpisi, ki urejajo njihovo obravnavo in varovanje. Pri tem gre zlasti za zakon, ki ureja varstvo tajnih podatkov, pa tudi za druge področne zakone, ki urejajo obravnavo in varovanje npr. davčne ali bančne tajnosti, posebnosti predpisov na področju zunanjih zadev, urejanje poslovne skrivnosti v skladu z zakonom, ki ureja gospodarske družbe in podobno. Izmenjava podatkov in informacij, ki so opredeljeni kot tajni ali poslovna skrivnost mora biti za potrebe izvajanja tega zakona v vsakem primeru 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.

Novost (glede na ZInfV) je določba tretjega odstavka predlaganega člena, ki določa pravila za izmenjavo podatkov in informacij, ki so varovani podatek pristojnega nacionalnega organa. Izmenjava podatkov in informacij, ki so varovani podatek pristojnega nacionalnega organa, mora biti za potrebe izvajanja tega zakona namreč 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 predlaga, da se varovani podatki pristojnega nacionalnega organa ne posredujejo javnosti.

Nadalje se s predlaganim četrtem odstavkom tega člena določa, da se pri posredovanju ali izmenjavi podatkov in informacij na podlagi tega zakona upošteva tudi sporazume o nerazkritju informacij in neformalne sporazume o nerazkritju informacij, kot je semaforski protokol, kar je novost glede na ZInfV, ki se v praksi, kot to navaja tudi uvodna izjava 9 Direktive (EU) 2022/2555/EU na koncu besedila, že uporablja v skoraj vseh skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter v nekaterih centrih za analizo in izmenjavo informacij. Kot to pojasnjuje navedena uvodna izjava je pri tem semaforski protokol (angl. *Traffic Light Protocol*) treba razumeti kot sredstvo za zagotavljanje informacij o kakršnih koli omejitvah v zvezi z nadaljnjim širjenjem informacij.

Ne glede na vse zgoraj opisane omejitve pri posredovanju ali izmenjavi zaupnih informacij pa peti odstavek prinaša še izrecno varovalko, po kateri 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. Tudi prej navedena uvodna izjava 9 navaja, da se od nobene države članice ne bi smelo zahtevati, da daje informacije, katerih razkritje bi bilo v nasprotju z bistvenimi (v našem pravnem redu se uporablja termin »vitalnimi«) interesi njene nacionalne varnosti, javne varnosti ali obrambe. Ocenjujemo, da je takšna izrecna varovalka potrebna, saj predlagani zakon ne izključuje njegove uporabe za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, kot je to pojasnjeno zgoraj v obrazložitvah k

1. ter zlasti k 2. členu predlaganega zakona. Vendar pa je ob ne izključitvi področja uporabe za zadevne subjekte hkrati treba upoštevati njihovo občutljivo naravo.

K 5. členu

V predlogu člena se pojasnjujejo uporabljeni izrazi; opredelitve izrazov so večinoma povzete po Direktivi (EU) 2022/2555 (njen 6. člen) oziroma se le-te deloma širijo zaradi načela minimalne harmonizacije iz 5. člena navedene direktive. V delu, ko gre za nacionalne določbe, pa se opredelitve pojmov zgledujejo po opredelitvah strokovnih pojmov s področja informacijske in kibernetske varnosti oziroma obramboslovja.

II. Zavezanci

V tem poglavju so navedeni zavezanci (za izpolnjevanje obveznosti) po predlaganem zakonu, ureja se mehanizem za njihovo samoregistracijo in podlaga za vodenje seznama zavezancev po tem zakonu.

K 6. členu

V predlogu člena se določajo zavezanci za izpolnjevanje obveznosti po predlaganem zakonu, Predlagani člen pri tem ob upoštevanju člena 5 Direktive 2022/2055 (minimalna harmonizacija) v predlagani zakon prenaša člen 3 Direktive 2022/2555 (bistveni in pomembni subjekti). Pri tem prvi odstavek predlaganega člena uvodno pojasnjuje, da se zavezanci delijo na bistvene in pomembne subjekte.

Predlog člena v drugem odstavku določa, da se za namene tega zakona šteje, da so bistveni subjekti: (1) subjekti vrste iz Priloge I, ki imajo vsaj 250 zaposlenih in letni promet vsaj 50 milijonov evrov ali letno bilančno vsoto vsaj 43 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; (6) subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo (7) subjekti, ki so bili v skladu z sedaj veljavnim Zakonom o informacijski varnosti (ZInfV)) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023; in (8) subjekti iz sektorja 9. Upravljanje storitev IKT iz Priloge I in niso subjekti iz točk 1 do 7 tega odstavka, ki jih na podlagi poimenskega seznama, ki ga pristojni organi po zakonu, ki ureja izvajanje Uredbe (EU) 2022/2554, posredujejo pristojnemu nacionalnemu organu, določi vlada. Pri prvih sedmih točkah gre za prenos določb oziroma možnosti iz prvega odstavka 3. člena Direktive (EU) 2022/2555 in sicer točk od (a) do (g) v predlagani zakon. Zadnja, to je 8. točka, je nacionalne narave in predstavlja dodatno možnost za določitev posameznega subjekta (ki spada v področje uporabe tega zakona po 3. členu predlaganega zakona) za bistveni subjekt, vendar na predlog pristojnih organov za izvajanje Uredbe (EU) 2022/2554 iz finančnega področja.

Tretji odstavek predlaganega člena v skladu drugim odstavkom 3. člena Direktive (EU) 2022/2555 določa pomembne subjekte, ki so subjekti vrste iz Prilog I ali II in drugi subjekti oziroma organi iz 3. člena predlaganega zakona, ki se ne štejejo za bistvene subjekte na podlagi prejšnjega odstavka. Gre torej za vse ostale subjekte, ki spadajo v področje uporabe predlaganega zakona in niso opredeljeni bistveni subjekti.

Četrti odstavek predlaganega člena izrecno določa, da Banka Slovenije ni zavezanec po tem zakonu ne glede na določbo 7. točke drugega odstavka tega člena, torej ne glede na njeno prejšnjo določitev za izvajalca bistvenih storitev po sedaj veljavnem ZInfV. Navedeno je skladu s položajem Banke Slovenije in namenom tako Direktive (EU) 2022/2555 kot tudi Uredbe (EU) 2022/2554.

Peti odstavek predlaganega člena določa, da določbe prvega, drugega in tretjega odstavka tega člena ne veljajo za druge fizične in pravne osebe iz dvanajstega odstavka 3. člena tega zakona, ki se za njih uporablja v delu, ki ureja certifikacijski okvir za kibernetsko varnost. Določba se torej nanaša na druge fizične in pravne osebe, ki niso bistveni ali pomembni subjekti po tem zakonu, ki jih zadeva Uredba (EU) 2019/881 v delu, ki ureja certifikacijski okvir za kibernetsko varnost.

K 7. členu

Predlog člena prenaša določbe tretjega, četrtega in petega odstavka 3. člena Direktive (EU) 2022/2555. 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. Države članice za namene priprave takšnega seznama od teh subjektov zahtevajo vsaj informacije naštete v četrtem odstavku prej navedene določbe, ki jih morajo subjekti tudi posodabljati po nastali spremembi, pri čemer države članice lahko vzpostavijo nacionalne mehanizme za samoregulacijo subjektov. Peti odstavek prej navedene določbe direktive pa pristojnim (nacionalnim) organom nalaga dolžnost in roke za obveščanje Evropske komisije o številu bistvenih in pomembnih subjektov, ki so na seznamu v posledici različnih določb navedene direktive. Šesti odstavek navedenega člena direktive pa daje možnost državam članicam, da lahko Evropsko komisijo na njeno zahtevo obveščajo tudi o imenih nekaterih takšnih subjektov, pri čemer takšna možnost v predlogu tega zakona ni bila uporabljena.

Predlog tega čelna prej navedene določbe Direktive (EU) 2022/2555 prenaša na način, da v prvem odstavku predlaganega člena najprej nalaga pristojnemu nacionalnemu organu, da vzpostavi mehanizem za samoregistracijo zavezancev iz prejšnjega (to je 6.) člena.

Drugi odstavek predlaganega člena nato nalaga zavezancem iz prejšnjega (to je 6.) člena predlaganega zakona, da se morajo registrirati preko mehanizma za samoregistracijo ter določa, katere informacije morajo ob tem podati. Pri tem se ob upoštevanju načela minimalne harmonizacije iz 5. člena Direktive (EU) 2022/2555 v interesu učinkovitejšega sodelovanja med pristojnim nacionalnim organom in zavezanci ter višanja ravni zagotavljanja informacijske in kibernetske varnosti nekoliko širi nabor informacij, ki jih kot minimalne določa Direktiva (EU) 2022/2555.

Tretji odstavek določa obveznost, da zavezanci nemudoma oziroma vsaj v dveh tednih sporočijo morebitne spremembe podatkov, ki so jih podali ob samoregistraciji.

Podlaga za vodenje seznama subjektov iz prvega odstavka predlaganega člena izhaja iz četrtega odstavka, ki določa, da pristojni nacionalni organ vzpostavi seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Do seznama imajo po predlogu petega dostavka dostop pristojne skupine CSIRT. Pristojni nacionalni organ Evropsko komisijo, v določenih primerih pa tudi Skupino za sodelovanje, obvešča o številu bistvenih in pomembnih subjektov.

Zaradi lažjega izvajanja oziroma upoštevanja določb 4. člena (Sektorski pravni akti Unije) Direktive (EU) 2022/2555, ki so sicer prenesene z devetim, desetim in enajstim odstavkom 3. člena predlaganega zakona, se na tem mestu predlaga, da organi, ki so pristojni za izvajanje področnih predpisov iz devetega odstavka 3. člena tega zakona, 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. Namreč področne predpise, kar vključuje tako neposredno uporabljive predpise EU, kot tudi morebitne nacionalne predpise, ki prenašajo EU zakonodajo ali pa so potrebni z vidika njenega

izvajanja v Republiki Sloveniji ter tudi zavezance za izpolnjevanje obveznosti po teh področnih predpisih najbolje poznajo organi, ki so pristojni za izvajanje takšnih področnih predpisov. Zato je najbolj primerno, da oni ustrezno obvestijo pristojni nacionalni organ, da ne bi v takšnih primerih prišlo do nepotrebnih nadzornih postopkov in sankcioniranja po predlaganem zakonu (morebiti že iz razloga, ker ni prišlo do samoregistracije takšnega subjekta). Pristojni nacionalni organ pa z organi pristojnimi za izvajanje takšnih področnih predpisov sodeluje na podlagi 5. točke 9. člena in 17. člena tega zakona.

III. Organizacija nacionalnega sistema informacijske varnosti

Poglavje vsebuje določbe glede strategije kibernetske varnosti, pristojnega nacionalnega organa (v nadaljnjem besedilu: PNO), enotne kontaktne točke, nacionalnega okvira za obvladovanje kibernetskih kriz in skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT). Za slednje določa zahteve in tehnične zmogljivosti ter njihove naloge in sodelovanje z deležniki zasebnega sektorja. To poglavje vsebuje tudi določbe o usklajenem razkrivanju ranljivosti in evropski podatkovni zbirki ranljivosti, sodelovanju na nacionalni ravni ter o. medsebojnem strokovnem pregledu.

K 8. členu

Predlog člena prenaša določbo 7. člena Direktive (EU) 2022/2555, ki določa, da vsaka država članica sprejme nacionalno strategijo, v kateri so opredeljeni strateški cilji, potrebna sredstva za dosego teh ciljev ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetske varnosti. Glede na navedeno so v predlogu člena določeni obveznost sprejetja strategije kibernetske varnosti, njena vsebina, namen in cilj. Elementi vsebine, ki jih mora strategija vsebovati, so taksativno našteti. Republika Slovenija že ima izdelano Strategijo kibernetske varnosti Republike Slovenije, ki jo je vlada sprejela 25. februarja 2016, bo pa po sprejetju predlaganega zakona to strategijo treba prilagoditi njegovim zahtevam. Tudi sicer je v predlogu zakona v prehodni določbi tretjega odstavka 59. člena predviden časovni okvir za sprejem strategije oziroma prilagoditev strategije določbam tega zakona (najkasneje v roku enega leta od uveljavitve tega zakona).

K 9. členu

Glede na zahteve 8. člena Direktive (EU) 2022/2555 je v predlaganem členu določen PNO.

V prvem odstavku je določeno, da je PNO Urad Vlade Republike Slovenije za informacijsko varnost.

V drugem odstavku je določeno, da PNO poleg drugih nalog, določenih v posameznih členih tega predloga zakona, izvaja še druge naloge in jih taksativno našteva, pri čemer gre za naloge, ki izhajajo tako iz Direktive (EU) 2022/2555 kot tudi takšne, ki so nacionalne narave. Pri tem na primer PNO koordinira delovanje nacionalnega sistema informacijske varnosti, razvija zmogljivosti za izvajanje kibernetske obrambe, vsem zavezancem pri izvajanju njihovih nalog nudi strokovno podporo, sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti in izvaja naloge mednarodnega sodelovanja.

K 10. členu

Glede na zahteve 8. člena Direktive (EU) 2022/2555 je v predlaganem členu s prvim odstavkom določena enotna kontna točka, ki je PNO. Člen obravnava vzpostavitev in vlogo enotne kontaktna točke, ki deluje kot ključni povezovalni organ med pristojnimi nacionalnimi organi ter med državami članicami EU, Evropsko komisijo in Evropsko agencijo za kibernetsko varnost (ENISA).

Ustanovitev enotne kontaktna točka: Prvi odstavek člena jasno določa, da je PNO določen kot enotna kontaktna točka v skladu z zakonom. Ta organ je odgovoren za koordinacijo in izvajanje nalog, povezanih s kibernetsko varnostjo na nacionalni ravni. Omenjeno nalogo je PNO opravljal tudi v skladu z obstoječim zakonom.

Povezovalna vloga enotne kontaktna točka: Drugi odstavek člena opisuje vlogo enotne kontaktne točke kot povezovalca med nacionalnimi organi in ustreznimi organi drugih držav članic EU, Evropsko komisijo in ENISA. S tem se zagotavlja čezmejno sodelovanje, izmenjavo informacij, koordinacijo ukrepov ter podporo pri reševanju kibernetskih incidentov in groženj.

Obveščanje Evropske komisije: Tretji odstavek člena določa obveznost PNO, da uradno obvesti Evropsko komisijo o določitvi enotne kontaktna točka, njenih nalogah ter ob vsakokratnih spremembah v zvezi s tem. To zagotavlja transparentnost in omogoča učinkovito čezmejno sodelovanje na ravni EU.

Skupaj ta člen vzpostavlja strukturo in vlogo enotne kontaktna točka kot ključnega elementa za koordinacijo in izboljšanje čezmejnega sodelovanja ter učinkovitega odzivanja na kibernetske grožnje in incidente med državami članicami EU ter relevantnimi institucijami EU. Gre za pomembno vlogo pri zagotavljanju skladnosti z evropskimi kibernetskimi standardi in smernicami ter pri izgradnji močnega kibernetskega varnostnega okolja na ravni EU.

Zavedati se moramo, da mednarodno sodelovanje prek enotne kontaktne točke vpliva na hitro izmenjava informacij med državami članicami in institucijami EU, ki je ključna za hitro prepoznavanje in odzivanje na kibernetske grožnje ter zagotavljanje učinkovitega odziva. Skupno obravnavanje kibernetskih incidentov omogoča združevanje virov, znanj in izkušenj za boljše obvladovanje in odpravljanje kibernetskih incidentov. Mednarodno sodelovanje prispeva k povečanju kibernetske varnosti z izmenjavo najboljših praks, tehnik odkrivanja in obrambnih strategij. Sodelovanje na mednarodni ravni omogoča boljše usklajevanje kibernetskih politik, standardov in zakonodaje med državami članicami. Redno mednarodno sodelovanje pa krepi zaupanje med državami in institucijami, kar je ključno za uspešno sodelovanje v boju proti kibernetskim grožnjam.

Zaradi naraščajočih kibernetskih groženj je mednarodno sodelovanje postalo nepogrešljiv element v strategiji kibernetske varnosti. Enotna kontaktna točka kot povezovalna točka igra ključno vlogo pri spodbujanju in olajšanju tega sodelovanja na ravni EU, s čimer prispeva k bolj odpornemu in varnemu kibernetskemu okolju tako na nacionalni kot tudi mednarodni ravni.

K 11. členu

Določbe 9. člena Direktive (EU) 2022/2555 zahtevajo, da vsaka država članica imenuje ali ustanovi enega ali več pristojnih organov, odgovornih za obvladovanje kibernetskih incidentov velikih razsežnosti in kibernetikih kriz (v nadaljnjem besedilu: organi za obvladovanje kibernetskih kriz). Člen obravnava vzpostavitev in delovanje organa za obvladovanje kibernetskih kriz v Republiki Sloveniji ter njegovo vlogo v obvladovanju kibernetskih incidentov, velikih razsežnosti in kibernetskih kriz.

Prvi odstavek člena določa, da je Urad Vlade Republike Slovenije za informacijsko varnost pristojni organ za obvladovanje kibernetskih incidentov velikih razsežnosti in kibernetskih kriz. Določa obveznost, da urad sodeluje v Evropski mreži organizacij za zvezo za kibernetske krize (mreža EU-CyCLONe), kar poudarja povezanost z mednarodnim okoljem.

Drugi odstavek člena navaja, da organ za obvladovanje kibernetskih kriz izdela nacionalni načrt odzivanja na kibernetske incidente, velike razsežnosti in krize. Ta načrt je usklajen z različnimi strategijami, načrti in varnostno dokumentacijo, kar zagotavlja celovit pristop k obvladovanju kibernetskih groženj.

Tretji odstavek člena podrobno opredeljuje vsebino nacionalnega načrta odzivanja, vključno z cilji, nalogami, postopki, ukrepi za pripravljenost, sodelovanjem med organi ter vključenimi deležniki. Ta

načrt zagotavlja strukturo in usmeritve za učinkovito obvladovanje kibernetskih incidentov na nacionalni ravni.

Četrti odstavek člena določa, da organ za obvladovanje kibernetskih kriz ob zaznavi kibernetskih incidentov, ki lahko povzročijo kibernetsko krizo, nemudoma obvesti Svet za nacionalno varnost. Sledi analiza situacije in predlog ukrepov za obvladovanje situacije.

Peti odstavek člena določa, da vlada lahko sprejme odločitev o vključitvi drugih državnih zmogljivosti v obvladovanje krize, razglasi krizo in izvaja krizno upravljanje v kompleksnih kriznih situacijah.

Šesti odstavek člena določa, da mora pristojni nacionalni organ obvestiti Evropsko komisijo o imenovanju organa za obvladovanje kibernetskih kriz ter predložiti informacije o nacionalnem načrtu odzivanja, pri čemer se izključijo informacije, ki bi lahko ogrozile interese nacionalne varnosti, javne varnosti ali obrambe Republike Slovenije.

Sedmi odstavek člena obravnava obveščanje javnosti v primeru potrebe, pri čemer pristojni nacionalni organ pripravi sporočilo za javno objavo v sodelovanju s službo vlade, pristojno za komuniciranje z javnostjo.

Skupaj ta člen vzpostavlja okvir za obvladovanje kibernetskih incidentov, velikih razsežnosti in kibernetskih kriz v Republiki Sloveniji, ki temelji na sodelovanju med različnimi organi, sektorji in mednarodnimi partnerji. Vključuje tudi jasne postopke za obveščanje in komuniciranje z javnostjo ter mednarodnimi partnerji, kar je ključno za učinkovito obvladovanje kibernetskih groženj na nacionalni in mednarodni ravni.

K 12. členu

V tem predlogu člena gre za prenos določb 10. Direktive (EU) 2022/2555 (skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT), ki se pri nekaterih svojih določbah sklicuje tudi na prvi odstavek 11 člena (Zahteve, tehnične zmogljivosti in naloge skupin CSIRT), na 19. člen (Medsebojni strokovni pregledi) in na 29. člen (Dogovori o izmenjavi o kibernetski varnosti) Direktive (EU) 2022/2555, kar je bilo upoštevano tudi v predlaganem členu, ki se na posamičnih mestih sklicuje na druge določbe predlaganega zakona, ki ustrezajo prenosu prej navedenih določb Direktive (EU) 2022/2555

V prvem odstavku predloga tega člena sta najprej določeni skupini CSIRT, ki sta CSIRT SI-CERT ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije ter CSIRT državne uprave (pojasnjujemo, da gre za CSIRT organov državne uprave po ZInfV), ki deluje kot notranja organizacijska enota SIGOV-CERT pri PNO. Skupini CSIRT delujeta kot odzivna centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Posledično opravljata koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah, ter izdajata opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih.

V drugem in tretjem odstavku je določena pristojnost posamezne skupine CSIRT za tam navedene skupine zavezanih subjektov.

Od petega do desetega odstavka predloga je urejeno področje izmenjave informacij, medsebojnega in mednarodnega sodelovanja.

Enajsti odstavek uvaja dolžnost obveščanja Evropske komisije o identiteti skupin CSIRT iz prvega odstavka tega člena ter njihovih nalogah iz drugega in tretjega odstavka tega člena, kot tudi o vsakokratnih spremembah o tem, pri čemer je PNO tisti, ki obvešča. Prav tako PNO obvesti Evropsko komisijo tudi o identiteti skupine CSIRT, ki je imenovana za koordinatorja iz prvega odstavka 16. člena tega zakona (usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti).

K 13. členu

V tem predlogu člena gre za prenos določbe prvega odstavka 11. člena Direktive (EU) 2022/2555. Predlog člena tako ureja zahteve in tehnične zmogljivosti, ki jih morata izpolnjevati skupini CSIRT. Tehnične zmogljivosti skupin CSIRT so ključne za zagotavljanje učinkovitega in usklajenega odziva na kibernetske grožnje ter varovanje kritične infrastrukture. Zahteve iz tega člena imajo svoj namen in prispevajo k celoviti zaščiti kibernetskega prostora.

Zagotavljanje visoke stopnje razpoložljivosti komunikacijskih kanalov: Varnostne incidente je treba obravnavati nemudoma, zato morajo skupine CSIRT zagotoviti visoko razpoložljivost svojih komunikacijskih kanalov. To vključuje preprečevanje ene same točke odpovedi, saj bi ta lahko povzročila zastoje ali zamude pri odzivu na incidente. Poleg tega je ključno, da so ti kanali jasno opredeljeni in da so uporabniki ter partnerji seznanjeni z njihovo uporabo, kar omogoča hitro in učinkovito komunikacijo v primeru varnostnih incidentov.

Nahajanje prostorov in informacijskih sistemov na varnih krajih: Fizična varnost je osnovna zahteva za zaščito informacijskih sistemov in podatkov skupin CSIRT. Nahajanje prostorov in informacijskih sistemov na varnih lokacijah zmanjšuje tveganje nepristojnega dostopa ali fizičnih napadov, s čimer se zagotavlja zaupnost in celovitost podatkov ter delovanje skupin v primeru fizičnih groženj.

Ustrezen sistem za upravljanje in usmerjanje zahtevkov: Enostavno in učinkovito upravljanje zahtevkov je ključno za hitro identifikacijo, analizo in odziv na varnostne incidente. Sistem za upravljanje zahtevkov mora omogočati učinkovito predajo zahtevkov med različnimi člani skupine CSIRT ter zagotavljati sledljivost in preglednost vseh aktivnosti.

Zagotovitev zaupnosti in zanesljivosti dejavnosti: Skupine CSIRT morajo delovati v skladu z najvišjimi standardi zaupnosti in zanesljivosti, da zagotovijo zaupanje uporabnikov in partnerjev. To vključuje uporabo ustrezne kriptografije, varnostnih postopkov in nadzornih mehanizmov za zaščito občutljivih podatkov ter preprečevanje morebitnih incidentov ali zlorab.

Dovolj osebja in ustrezno usposabljanje: Za zagotavljanje neprekinjene razpoložljivosti storitev je bistvenega pomena, da skupine CSIRT razpolagajo z zadostnim številom usposobljenega osebja. Prav tako je pomembno, da je to osebje ustrezno usposobljeno za obravnavo različnih vrst varnostnih incidentov ter za uporabo in vzdrževanje specializirane varnostne opreme in tehnologij.

Redundantni sistemi in nadomestni delovni prostor: Zaradi narave kibernetskih groženj in možnosti izpada ključnih sistemov je pomembno, da skupine CSIRT razpolagajo z redundantnimi sistemi ter načrti za obnovitev dejavnosti v primeru izrednih dogodkov. Redundantni sistemi omogočajo nadaljevanje operacij tudi v primeru okvar ali izpadov, medtem ko nadomestni delovni prostor omogoča prehod na alternativne lokacije za izvajanje operativnih dejavnosti v primeru nepredvidenih situacij.

Skladno s prenosom NIS 2 direktive je izpolnjevanje teh zahtev ključno za zagotavljanje učinkovitega odziva na kibernetske grožnje ter zaščito kritične infrastrukture in podatkovnih virov.

Ob tem je treba opozoriti, da je le dosedanji nacionalni CSIRT, pri čemer gre za odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri javnem zavodu Arnes, na podlagi tretjega odstavka 28. člena ZInfV že moral izpolnjevati zahteve glede visoke stopnje razpoložljivosti svojih storitev, varnosti svojih poslovnih prostorov ter neprekinjenega poslovanja skladno z Direktivo 2016/1148/ES, pojasnjujemo, da je takšne zahteve določala Priloga I prej navedene direktive. Zato se bodo glede na zahteve le prilagodili glede na zahteve iz Direktive (EU) 2022/2555, v kolikor takšne zahteve še niso v celoti izhajali iz Direktive 2016/1148/ES, na katero se sklicuje tretji odstavek 28. člena ZInfV.

K 14. členu

V tem predlogu člena gre za prenos določbe tretjega odstavka 11. člena Direktive (EU) 2022/2555, ki določa naloge skupin CSIRT.

Prvi odstavek predlaganega člena taksativno našteje naloge obeh skupin CSIRT, ki jih morata izvajati.

V drugem odstavku predlog določa pristojnost, da skupini CSIRT lahko izvajata proaktivno in nevsiljivo pregledovanje javno dostopnih omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov, za katere je pristojna.

S predlaganim tretjim odstavkom se skupinama CSIRT omogoča, da lahko pri izvajanju nalog iz prvega odstavka predlaganega člena prednostno razvrstita nekatere naloge na podlagi pristopa, ki temelji na tveganjih.

V četrtem odstavku predloga je navedena obveznost izdelave tedenskega in četrtletnega poročila o izvajanju svojih nalog, ki ga morata skupini CSIRT posredovati PNO.

V petem odstavku predloga je predvidena obveznost nacionalne narave, da skupina CSIRT obvesti PNO o lastnem incidentu, ki bi lahko vplival ali vpliva na delovanje in razpoložljivost njihovih storitev, ki jih nudijo zavezancem in prostovoljnim priglasiteljem.

Po predlaganem šestem odstavku, ki je nacionalne narave, skupina CSIRT v skladu z usmeritvami pristojnega nacionalnega organa v primeru razglasitve ocene ogroženosti visoko ali kritično izda varnostno obvestilo ali navodilo v skladu s petim in šestim odstavkom 33. člena tega zakona.

Tudi predlagana sedmi in osmi odstavek sta nacionalne narave in nudita dodatno potrebna pooblastila CSIRT-u državne uprave, pri čemer določbi vsebinsko ustrezata obstoječim določbam tretjega in četrtega odstavka 29. člena veljavnega ZInfV. Po navedenih določbah ZInfV je CSIRT organov državne uprave že doslej in z enakimi nameni, kot je to ponovno določeno za CSIRT državne uprave v tem predlogu, pooblaščen za neposredni, nujni in sorazmerni vpogled v delovanje informacijske infrastrukture centralnega informacijsko-komunikacijskega sistema, upravljavec centralnega informacijsko-komunikacijskega sistema pa mu mora to omogočiti kot tudi, da upravljavcu centralnega informacijsko-komunikacijskega sistema oziroma povezanim subjektom odredi ustrezne, nujne in sorazmerne ukrepe, ki jih morajo ti nemudoma oziroma v postavljenem roku izvesti v svojem informacijsko-komunikacijskem sistemu.

Deveti odstavek predloga določa, da skupini CSIRT lahko izvajata tudi programe ozaveščanja v skladu s Strategijo kibernetske varnosti.

K 15. členu

V tem predlogu člena gre za prenos določbe četrtega in petega odstavka 11. člena Direktive (EU) 2022/2555, ki za dosego ciljev določa vzpostavitev sodelovanje z ustreznimi deležniki iz zasebnega sektorja.

V prvem odstavku predloga je predvideno sodelovanje skupin CSIRT z ustreznimi deležniki iz zasebnega sektorja.

Drugi odstavek predloga pa določa način in namen sodelovanja ter taksonomijo.

Tretji odstavek predloga pa nalaga skupini CSIRT, ki zazna ranljivost informacijsko-komunikacijskega sistema, da mora o tem brez nepotrebnega odlašanja obvestiti skrbnika sistema.

K 16. členu

V tem predlogu člena gre za prenos določbe 12. člena Direktive (EU) 2022/2555, ki vpeljuje rešitev usklajenega razkrivanja ranljivosti in evropsko podatkovno zbirko ranljivosti.

Prvi odstavek predloga določa, da je koordinator za usklajeno razkrivanje ranljivosti v Republiki Sloveniji (v nadaljnjem besedilu koordinator) skupina CSIRT SI-CERT. Koordinator olajšuje sodelovanje med fizično ali pravno osebo, ki poroča o ranljivostih, in proizvajalcem ali ponudnikom proizvodov IKT ali storitev IKT, ki naj bi zajemali ranljivost, in sicer na pobudo katere koli stranke. Pojasnjujemo, da SI-CERT omenjeno nalogo že samoiniciativno opravlja od oktobra 2023.

Drugi odstavek predloga določa naloge koordinatorja. Tretji odstavek predloga omogoča, da fizične ali pravne osebe lahko koordinatorju o ranljivostih poročajo anonimno. Koordinator po potrebi sodeluje z drugimi skupinami CSIRT, ki so imenovane za koordinatorke v okviru mreže skupin CSIRT. Četrti odstavek predloga nalaga koordinatorju sodelovanje z ENISO, ki vodi evropsko podatkovno zbirko ranljivosti. Pet, šesti, sedmi in osmi odstavek predloga določa vzpostavitev nacionalne zbirke ranljivosti ter sodelovanje med koordinatorjem in pristojnim nacionalnim organom.

K 17. členu

V tem predlogu člena gre za prenos določbe 13. člena Direktive (EU) 2022/2555 o sodelovanju na nacionalni ravni.

Prvi odstavek predloga za zagotovitev učinkovitega opravljanja nalog in obveznosti pristojnega nacionalnega organa, enotne kontaktne točke in skupin CSIRT določa, da se vzpostavi ustrezno sodelovanje na nacionalni ravni. Oblike sodelovanja se izvajajo na način, da medsebojno sodelujejo pri izpolnjevanju obveznosti; da sodelujejo z organi kazenskega pregona, Informacijskim pooblaščencem, Javno agencijo za civilno letalstvo Republike Slovenije, Inšpekcijo za informacijsko družbo, Banko Slovenije, Agencijo za komunikacijska omrežja in storitve Republike Slovenije in pristojnim organom iz zakona, ki ureja kritično infrastrukturo ter pristojnimi organi oziroma sektorskimi regulatorji iz drugih področnih zakonov iz področij, ki jim pripadajo zavezanci iz 6. člena tega zakona; da redno sodelujejo s pristojnim organom iz zakona, ki ureja kritično infrastrukturo in si izmenjujejo informacije o identifikaciji kritičnih subjektov, o tveganjih, kibernetskih grožnjah in incidentih, pa tudi o nekibernetskih tveganjih, grožnjah in incidentih, ki vplivajo na bistvene subjekte, ki so opredeljeni kot kritični subjekti na podlagi zakona, ki ureja kritično infrastrukturo, ter o ukrepih, sprejetih v odziv na takšna tveganja, grožnje in incidente ter redno izmenjujejo informacije, tudi o relevantnih incidentih in kibernetskih grožnjah z Inšpekcijo za informacijsko družbo, Banko Slovenije, Javno agencijo za civilno letalstvo Republike Slovenije in Agencijo za komunikacijska omrežja in storitve Republike Slovenije.

Drugi odstavek predloga določa obveznost medsebojne izmenjava informacij o incidentih, kibernetskih grožnjah in skorajšnjih incidentih. Za ta namen PNO vzpostavi digitalno platformo.

Tretji odstavek predloga pa določa, da za potrebe nacionalnega sistema za zagotavljanje informacijske varnosti lahko pristojni nacionalni organ in skupine CSIRT sodelujejo s subjekti v javni upravi, gospodarstvu, z raziskovalno-razvojnimi organizacijami, znanstvenimi institucijami, interesnimi združenji in posamezniki. Gre za določbo, ki jo ohranjamo iz obstoječega Zakona o informacijski varnosti (30. člen).

K 18. členu

V tem predlogu člena gre za prenos določbe 19. člena Direktive (EU) 2022/2555 o medsebojnih strokovnih pregledih.

Prvi odstavek predloga določa, da PNO lahko odloči, da z namenom učenja iz skupnih izkušenj, okrepitve medsebojnega zaupanja, doseganja visoke skupne ravni kibernetske varnosti ter okrepitve zmogljivosti in politike na področju kibernetske varnosti, pristopi k medsebojnim strokovnim pregledom, ki jih izvajajo imenovani strokovnjaki s področja kibernetske varnosti drugih držav članic Evropske unije. Evropske komisija in ENISA sodelujeta v medsebojnih strokovnih pregledih kot opazovalki. Drugi odstavek predloga določa področja medsebojnih strokovnih pregledov. Tretji odstavek predloga določa, da se uporablja metodologija, ki jo pripravi Skupina za sodelovanje s

pomočjo Evropske komisije in ENISA ter po potrebi mreža skupin CSIRT. Četrti odstavek predloga določa postopke pred začetkom medsebojnega strokovnega pregleda. PNO lahko v skladu s petim odstavkom predloga pred začetkom medsebojnega strokovnega pregleda izvede samooceno vidikov, ki bodo pregledani. Šesti odstavek predloga določa obseg medsebojnih strokovnih pregledov, med tem ko sedmi odstavek predloga omejuje uporabo informacij pridobljenih v okviru medsebojnega strokovnega pregleda. Osmi odstavek predlog določa način izbire strokovnjakov. PNO lahko v skladu z devetim odstavkom predloga lahko nasprotuje imenovanju posameznih strokovnjakov. V skladu z desetim odstavkom predloga strokovnjaki za kibernetsko varnost, ki sodelujejo v medsebojnih strokovnih pregledih, pripravijo poročila o ugotovitvah. PNO lahko v skladu z enajstim odstavkom predloga predloži pripombe na osnutek poročila, ter se lahko odloči, da naredi poročilo javno ali njegovo redigirano različico javno dostopno.

IV. Ukrepi za obvladovanje tveganj in priglasitve incidentov

Poglavje vsebuje določbe glede upravljanja, varnostne dokumentacije in ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, obveze posredovanja podatkov in informacij, certifikacijske sheme za kibernetsko varnost, standardizacije in obveznosti priglašanja in obveščanja. Določa tudi postopek priglasitve pomembnih incidentov.

K 19. členu

V tem predlogu člena gre za prenos določbe 20. člena Direktive (EU) 2022/2555 o upravljanju.

Prvi odstavek predloga določa, da so odgovorne osebe pravnih oseb oziroma člani poslovodnih organov bistvenega ali pomembnega subjekta, odgovorne za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v skladu z določbami tega zakona. Drugi odstavek predloga določa, da morajo odgovorne osebe odobriti ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih subjekt izvaja zaradi izpolnjevanja obveznosti, določenih s tem zakonom in nadzirati njihovo izvajanje. Tretji odstavek predloga pa nalaga odgovorni osebi, da se mora izobraževati oziroma usposabljati na področju obvladovanja tveganj kibernetske varnosti in njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt. Odgovorne osebe po predlogu četrtega odstavka morajo zagotoviti 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. Peti odstavek predloga določa, da mora odgovorna oseba zagotoviti, 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.

K 20. členu

Trenutno veljavni ZInfV zavezance deli na organe državne organe, izvajalce bistvenih storitev, ponudnike digitalnih storitev in povezane subjekte, pri čemer ima vsaka kategorija subjekta skupni člen, v katerem so opredeljeni varnostna dokumentacija in ukrepi. Predlog novega ZInfV v skladu z Direktive (EU) 2022/2555 določa le dve kategoriji zavezancev in sicer bistvene in pomembne subjekte. Dokumentacija in varnostni ukrepi sta razdeljena v dva člena, pri čemer 20. člen določa varnostno dokumentacijo (21. člen pa varnostne ukrepe).

Prvi odstavek določa obvezno varnostno dokumentacijo, ki jo morata imeti obe kategoriji subjektov, torej tako bistveni kot pomembni. Predlog jim nalaga obveznost vzpostavitve in vzdrževanja dokumentiranega sistema upravljanja varovanja informacij, ki ima najmanj sedem obveznih sestavin

(točke 1. do 7.). V veliki meri je dokumentacija podobna sedaj obvezni (12. in 17. člen ZInfV), pri čemer so dodani še elementi iz 21. člena Direktive (EU) 2022/2555.

Drugi odstavek zavezancem nalaga, da morajo določiti obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja na podlagi rezultatov analize vpliva na poslovanje (angl. BIA – Business Impact Analysis). Šele z opravljeno analizo vpliva na poslovanja lahko namreč subjekti realno ocenijo in določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja.

Tretji odstavek določa, da subjektom, ki že imajo izdelano dokumentacijo na podlagi drugih predpisov, ni potrebno izdelati celotne dokumentacije na novo, temveč le obstoječo dopolnijo tako, da je skladna s tem zakonom.

Četrti odstavek daje Vladi Republike Slovenije možnost, da s podzakonskim aktom bolj podrobno uredi vsebino in strukturo varnostne dokumentacije, pri čemer upošteva tudi dokumente in priporočila ENISA.

K 21. členu

Predlagani člen določa varnostne ukrepe, ki jih je zavezanec dolžan sprejeti in izvajati na podlagi vsebine dokumentacije iz 20. člena.

Prvi odstavek obema kategorijama subjektom nalaga obveznost sprejetja ukrepov za zagotavljanje t. i. »CIA triade« (zaupnost, integriteta, razpoložljivost), s katerimi obvladujejo tveganja za varnost sistemov, ki jih uporabljajo pri svojem delovanju z namenom, da se čim bolj zmanjša vpliv morebitnih incidentov na uporabnike storitev.

V drugem odstavku je naštetih 16 splošnih ukrepov za zagotavljanje CIA, ki so delno povzeti iz Direktive (EU) 2022/2555 (drugi odstavek 21. člena), delno pa iz obstoječega ZInfV, ki morajo temeljiti na pristopu upoštevanja vseh groženj oziroma nevarnosti (okoljske, fizične, kibernetske grožnje, ipd.).

Tretji odstavek določa, katere elemente morajo subjekti upoštevati pri izvedbi varnostnih ukrepov iz drugega odstavka.

Četrti odstavek določa način hrambe dnevniških zapisov. Gre za rešitev iz obstoječega zakona, ki se je izkazala kot potrebna in pomembna za dvig kibernetske varnosti zavezancev.

Peti odstavek bolj natančno opredeljuje kriterije, ki jih morajo subjekti upoštevati pri oceni in izvedbi ukrepov, ki se nanašajo na varnost dobavne verige (21. in 22. člen Direktive (EU) 2022/2555).

Šesti odstavek subjekte zavezuje k rednemu periodičnemu preverjanju izpolnjevanja varnostnih ukrepov iz tretjega odstavka tega člena in določa obveznosti v primeru odkritih pomanjkljivosti.

V sedmi odstavek se prenaša peti odstavek 21. člena Direktive (EU) 2022/2555, ki zavezuje kategorije ponudnikov in registrov, da pri sprejemu varnostnih ukrepov upoštevajo izvedbene akte EK, ki so določeni v petem odstavku 21. člena Direktive (EU) 2022/2555. Evropska komisija namreč lahko sprejme izvedbene akte, s katerimi določi tehnične in metodološke zahteve, ki jih bodo morale kategorije ponudnikov in registrov upoštevati.

Ostali subjekti, ki niso navedeni v prejšnjem odstavku, morajo v skladu s predlogom osmega odstavka tega člena upoštevati morebitne druge izvedbene akte Evropske komisije, s katerimi določi tehnične in metodološke zahteve za varnostne ukrepe.

V predlogu devetega odstavka se uvaja prepoved, po kateri bistveni in pomembni subjekti ne smejo uporabljati informacijsko-komunikacijskih rešitev, ki imajo aktivno izkoriščane ranljivosti, brez dodatne izvedbe ocene tveganja in uvedbi dodatnih ukrepov, ki znižajo stopnjo tveganja na sprejemljivo raven.

Deseti odstavek bistvenim in pomembnih subjektom nalaga dodatne obveznosti, če za opravljanje svoje dejavnosti črpajo vhodne podatke in informacije iz ključnih delov nacionalno varnostnega

sistema. Za vzpostavitev zahtev v tem primeru s predlagano določbo potrebujejo soglasje pristojnega ministrstva ali vladne službe za posamezni ključni del nacionalno varnostnega sistema.

Enajsti odstavek Vladi RS omogoča sprejem podzakonskega akta, s katerim lahko podrobneje določi način izvajanja obveznosti iz tega člena, pri čemer upošteva tudi morebitne dokumente in priporočila ENISA.

Zadnji odstavek se nanaša na centralni informacijsko-komunikacijski sistem (HKOM) in upravljavcu nalaga obveznosti, ki se nanašajo na subjekte, ki se povezujejo v HKOM ter upravljavcu daje pooblastila za določitev varnostnih zahtev za priklop v omrežje in izvedbo nujnih ukrepov, ki se nanašajo na zaščito HKOM omrežja in infrastrukture (npr. začasni odklop subjekta iz HKOM v primeru nesprejemljivih ravnanj oziroma tveganj).

K 22. členu

V tem predlogu člena gre za nacionalno določbo, ki določa obveza posredovanja podatkov in informacij. Gre za rešitev iz obstoječega zakona, ki se je izkazala kot pomembna za dvig kibernetske varnosti zavezancev. Člen obravnava obveznosti bistvenih in pomembnih subjektov glede izmenjave informacij s pristojnim nacionalnim organom v kontekstu zakona. Poudarja pomen sodelovanja med subjekti in organom ter zagotavljanje učinkovitega izvajanja zakonskih pristojnosti.

Obveznost izmenjave informacij: Prvi odstavek člena jasno določa, da morajo bistveni in pomembni subjekti pristojnemu nacionalnemu organu posredovati potrebne podatke in informacije na podlagi pisne zahteve. To pomeni, da morajo subjekti aktivno sodelovati z organom, da omogočijo izvajanje pristojnosti organa v skladu z zakonom. Ta obveznost je ključna za zagotavljanje učinkovitega nadzora, upravljanja in izvajanja zakonskih določb v zvezi s kibernetsko varnostjo.

Načelo sorazmernosti: Drugi odstavek člena postavlja pomembno omejitev glede vrste in obsega zahtevanih informacij. Zahtevani podatki in informacije morajo biti sorazmerni namenu, za katerega bodo uporabljeni. To pomeni, da pristojni nacionalni organ ne sme zahtevati več informacij, kot je potrebno za izpolnitev svojih zakonskih pristojnosti. Ta načelo varuje subjekte pred nepotrebnim razkritjem občutljivih informacij in zagotavlja, da je izmenjava informacij uravnotežena in razumna.

Transparentnost in jasnost zahtev: Pristojni nacionalni organ mora v svoji zahtevi natančno navesti namen uporabe zahtevanih podatkov in informacij. To zagotavlja, da subjekti jasno razumejo, zakaj so določene informacije potrebne, in lahko ocenijo, ali je zahteva upravičena in sorazmerna.

Skupaj ta člen vzpostavlja jasna pravila in smernice za izmenjavo informacij med bistvenimi in pomembnimi subjekti ter pristojnim nacionalnim organom. Z obveznostjo sodelovanja, načelom sorazmernosti in zahtevo po jasnosti namena se zagotavlja uravnotežen pristop k zbiranju in uporabi informacij v kontekstu kibernetske varnosti.

K 23. členu

V tem predlogu člena gre za prenos določbe 24. Direktive (EU) 2022/2555, ki določa certifikacijske sheme za kibernetsko varnost. Predlog obravnava okvir izvajanja evropskih certifikacijskih shem za kibernetsko varnost v skladu z Uredbo (EU) 2019/881, določa pristojni nacionalni certifikacijski organ za kibernetsko varnost ter nacionalni akreditacijski organ in njune naloge v zvezi z evropsko certifikacijsko shemo, opredeljuje vlogo organov za ugotavljanje skladnosti in organ, ki jih akreditira; opredeljuje obravnavanje pritožb glede izdanih evropskih certifikatov kibernetske varnosti; - zavezancem na podlagi tega zakona napotuje k prednostni uporabi proizvodov IKT, storitev IKT ali postopkov IKT, ki so prestali presojo skladnosti glede pravil, tehničnih zahtev, standardov in postopkov, ki so vzpostavljeni na ravni Unije in se uporabljajo za certificiranje ali ugotavljanje skladnosti posameznih proizvodov IKT, storitev IKT ali postopkov IKT.

Predlog člena obravnava evropski certifikacijski okvir za kibernetsko varnost, certificiranje ali ugotavljanje skladnosti v skladu z evropskimi certifikacijskimi shemami. Evropski certifikacijski okvir in zahteve za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost določa Uredba (EU) 2019/881. Namen certificiranja in ugotavljanje skladnosti je zagotavljanje ustrezne ravni kibernetske varnosti za proizvode IKT, storitve IKT ali postopke IKT, še posebej kadar jih uporabljajo zavezanci po tem zakonu. Evropski certifikat kibernetske varnosti, ki ga izda akreditiran organ za ugotavljanje skladnosti pomeni, da je bil zadevni proizvod IKT, storitev IKT ali postopek IKT ocenjen glede skladnosti s posebnimi varnostnimi zahtevami, določenimi v evropski certifikacijski shemi za kibernetsko varnost. Organe za ugotavljanje skladnosti oz. certifikacijski organ akreditira nacionalni akreditacijski organ.

Evropska certifikacijska shema za kibernetsko varnost lahko določa eno ali več naslednjih ravni zanesljivosti za proizvode IKT, storitve IKT in postopke IKT: „osnovno“, „znatno“ ali „visoko“. Raven zanesljivosti ustreza stopnji tveganja, povezani s predvideno uporabo proizvoda IKT, storitve IKT ali postopka IKT v smislu verjetnosti nastanka in velikosti posledic incidenta. Evropska certifikacijska shema dopušča tudi samoocenjevanje skladnosti, ki ga izvede proizvajalec IKT oziroma ponudnik IKT, s čimer, s podpisom dokumenta - izjave EU o skladnosti prevzame odgovornost za skladnost proizvoda IKT, storitve IKT in postopka IKT z zahtevami evropske certifikacijske sheme za kibernetsko varnost. Izjava EU o skladnosti in samoocenjevanje se lahko nanaša samo za produkte IKT storitve IKT, ki predstavljajo nizko tveganje za javni interes, kot so preprosta zasnova in mehanizmi proizvodnje.

Predlog zakona v skladu Uredbo (EU) 2019/881 določa, da izdajanje certifikata za visoko raven zanesljivosti lahko izda samo nacionalni certifikacijski organ za kibernetsko varnost oziroma organ za ugotavljanje skladnosti, na katerega je pristojni nacionalni organ prenesel pooblastilo izdajanja evropskih certifikatov kibernetske varnosti.

V predlogu zakona nalogo nacionalnega certifikacijskega organa za kibernetsko varnost ohranja Urad Vlade RS za informacijsko varnost, vlogo nacionalnega akreditacijskega organa pa Slovenska akreditacija, ki je v skladu z Zakonom o akreditaciji (Uradni list RS, št. 59/99) s pooblastilom države edina, neodvisna in nepridobitna institucija, ki opravlja naloge nacionalne akreditacijske službe v Sloveniji. Naloge nacionalnega certifikacijskega organa za kibernetsko varnost ter naloge in zahteve glede organov za ugotavljanje skladnost že določa Uredba (EU) 2019/881.

Predlog zakona tudi naslavlja pritožbe fizičnih in pravnih oseb glede izdanih evropskih certifikatov kibernetske varnosti ter postopek obravnave le-teh.

Zaradi zagotavljanja višje ravni kibernetske varnosti in z namenom zagotovitve skladnosti z nekaterimi zahtevami iz 20. člena, predlog zakona spodbuja bistvene in pomembne subjekte, da uporabljajo kvalificirane storitve zaupanja ter uporabljajo proizvode IKT, storitve IKT in postopke IKT, ki so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost. Izjema so subjekti iz kategorij, ki jih določi Evropska komisija z delegiranim aktom, ki morajo za obvladovanje tveganj za kibernetsko varnost uporabljati v njem določene certificirane proizvode IKT, storitve IKT in procese IKT ali pridobiti certifikat na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49 Uredbe (EU) 2019/881.

Predlog zakona zavezance zakona spodbuja, da prednostno uporabljajo tudi tiste proizvode IKT, storitve IKT ali postopke IKT, kjer je proizvajalec ali ponudnik izdal in podpisal izjavo EU o skladnosti proizvoda IKT, storitve IKT ali postopka IKT oziroma je ugotavljanje skladnosti proizvoda IKT, storitve IKT ali postopka IKT z zahtevami evropskih certifikacijskih shem za kibernetsko varnost izvedel kateri izmed organov za ugotavljanje skladnosti držav članic EU.

Predlog zakona predvideva, da lahko vlada zaradi potrebe po višji ravni kibernetske varnosti iz razlogov zagotavljanja nacionalne varnosti, določenim kategorijam bistvenih subjektov predpiše obvezno uporabo certificiranih proizvodov IKT, storitev IKT ali postopkov IKT, vključno z določitvijo raven zanesljivosti, ki jo morajo izpolnjevati glede na stopnjo tveganja in predvideno uporabo.

K 24. členu

V tem predlogu člena gre za prenos določbe 25. člena Direktive (EU) 2022/2555, ki določa standardizacijo. Gre za rešitev, ki je že uveljavljena z 19. členom obstoječega zakona. Člen obravnava pomembnost standardizacije v kontekstu varnosti omrežnih in informacijskih sistemov. Standardizacija je ključni element za zagotavljanje skladnosti in učinkovitega izvajanja varnostnih ukrepov v informacijski tehnologiji.

Bistveni in pomembni subjekti, ki so odgovorni za varnost omrežij in informacijskih sistemov, dolžni uporabljati evropske in mednarodne standarde ter tehnične specifikacije. To pomeni, da morajo upoštevati uveljavljene industrijske standarde in najboljše prakse pri razvoju, implementaciji in vzdrževanju svojih sistemov. Standardi in tehnične specifikacije, ki obravnavajo varnost omrežij in informacijskih sistemov, so ključni za preprečevanje kibernetskih groženj, kot so napadi, zlorabe in kršitve podatkov. Z upoštevanjem teh standardov subjekti zagotavljajo, da so njihovi sistemi zaščiteni in odporni proti različnim varnostnim tveganjem. Evropska agencija za kibernetsko varnost (ENISA) je pomembna institucija, ki izdaja smernice in nasvete glede varnosti omrežij in informacijskih sistemov. Upoštevanje njenih smernic je ključno za zagotavljanje skladnosti z evropskimi standardi in najboljšimi praksami na področju kibernetske varnosti. Pristojni nacionalni organ ima vlogo pri osveščanju in informiranju zavezancev o uporabi ustreznih standardov in tehničnih specifikacij. Pristojni nacionalni organ je odgovoren za zagotavljanje, da so subjekti seznanjeni z veljavnimi standardi in da jih ustrezno uporabljajo.

Skupaj ta člen poudarja pomen standardizacije kot sredstva za izboljšanje kibernetske varnosti in zagotavljanje skladnosti z zakonodajo na področju informacijske tehnologije. Standardi in tehnične specifikacije služijo kot temelj za razvoj varnih in zanesljivih informacijskih sistemov, medtem ko vloge ENISA in nacionalnih organov zagotavljajo, da so ti standardi ustrezno razumljeni, uporabljeni in upoštevani.

Na področju informacijske oziroma kibernetske varnosti se uporabljajo različni standardi, ki določajo najboljše prakse in smernice za varovanje informacijskih sistemov, omrežij in podatkov. Nekateri izmed najbolj znanih standardov vključujejo:

- ISO/IEC 27001, mednarodni standard za upravljanje informacijske varnosti, ki določa zahteve za vzpostavitev, izvajanje, vzdrževanje in izboljšanje sistema upravljanja informacijske varnosti v organizacijah;

- ISO/IEC 27002, standard ponuja smernice in najboljše prakse za izvajanje ukrepov iz ISO/IEC 27001. Pokriva širok spekter tem, vključno z varnostnimi politikami, organizacijsko varnostjo, upravljanjem sredstev, dostopom, kriptografijo, fizično varnostjo in drugimi;

- NIST Cybersecurity Framework: Razvit s strani Nacionalnega inštituta za standarde in tehnologijo (NIST) v ZDA, ta okvir ponuja prilagodljiv pristop k vzpostavitvi, izboljšanju in upravljanju kibernetske varnosti;

- CIS Controls (Center for Internet Security Controls), nabor kontrol, ki so namenjene izboljšanju varnosti informacijskih sistemov. Kontrole so organizirane v obliki seznama najpomembnejših ukrepov za izboljšanje kibernetske varnosti;

- GDPR (Splošna uredba o varstvu podatkov): čeprav ni standard v klasičnem smislu, GDPR določa zahteve za zaščito osebnih podatkov državljanov EU, kar je pomembno za informacijsko varnost.

Standarde in okvire pogosto uporabljajo organizacije za vzpostavitev in vzdrževanje učinkovitih varnostnih programov, ki zagotavljajo zaščito pred kibernetskimi grožnjami. Izbor ustreznih standardov pa je odvisen od vrste organizacije, njenih poslovnih potreb in sektorskih regulativnih zahtev, s katerimi se sooča.

K 25. členu

V tem predlogu člena gre za prenos določb prvega, drugega in tretjega odstavka 23.člena Direktive (EU) 2022/2555, ki določa obveznost priglašanja in obveščanja.

Prvi odstavek predloga določa, da bistveni in pomembni subjekti pristojni skupini CSIRT brez nepotrebnega odlašanja priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Odstavek tudi definira kaj se šteje za pomemben incident.

Drugi odstavek predloga določa, da se upoštevajo morebitni izvedbeni akti Evropske komisije, s katerimi ta podrobneje določi vrsto informacij, obliko in postopek priglasitve ter prostovoljne priglasitve in obvestila.

Tretji odstavek predloga določa, da 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, kot tudi ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, pri priglašanju upoštevajo izvedbene akte Evropske komisije, v katerih so zanje podrobneje določeni primeri, ko se incident šteje za pomembnega. Četrti odstavek predloga za ostale bistvene in pomembne subjekte določa, da upoštevajo morebitne izvedbene akte Evropske komisije. Če Evropska komisija takšnih izvedbenih aktov ne sprejme, se za te subjekte upošteva metodologija za določitev pomembnosti incidenta, kot je opredeljena v nacionalnem načrtu odzivanja.

Peti odstavek predloga nalaga katere informacije morajo posredovati bistveni in pomembni subjekti pristojni skupini CSIRT. Določa tudi postopek posredovanja informacije enotni kontaktni točki.

Šesti odstavek predloga obvezuje bistvene in pomembne subjekte, da brez nepotrebnega odlašanja uradno obvestijo prejemnike svojih storitev o pomembnih incidentih, ki bodo verjetno negativno vplivali na zagotavljanje teh storitev.

Sedmi odstavek predloga pa bistvene in pomembne subjekte zavezuje, da brez nepotrebnega odlašanja prejemnikom svojih storitev, ki bi jih pomembna kibernetska grožnja lahko prizadela, sporočijo vse ukrepe ali sredstva, ki jih lahko ti prejemniki sprejmejo v odziv na to grožnjo.

K 26. členu

V tem predlogu člena gre za prenos določb četrtega odstavka 23.člena Direktive (EU) 2022/2555, ki določa obveznost poročanja oziroma postopek priglasitve pomembnih incidentov. Prenašajo se tudi tretji in šesti odstavek 13. člena Direktive (EU) 2022/2555

Prvi odstavek predloga določa kaj morajo bistveni in pomembni subjekti za namen priglasitve pomembnih incidentov predložiti in poročati pristojni skupini CSIRT.

Drugi odstavek predloga določa posebno zahtevo za ponudnike storitev zaupanja v zvezi s pomembnimi incidenti, ki vplivajo na zagotavljanje njegovih storitev.

Tretji odstavek predloga nalaga postopek odzivanja skupine CSIRT po prejeti priglasitvi, ki vključuje odgovor priglasitvenemu subjektu, seznanitev PNO ter usmeritve o poročanju organom kazenskega pregona.

Četrti odstavek predloga določa postopek v primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta. Pri obveščanju prek enotne kontaktne točke v skladu s pravom Evropske unije ali pravom Republike Slovenije zaščiti varnost in poslovne interese zavezanca ter zaupnost predloženih informacij, ki jih slednji zagotovi v svoji priglasitvi.

Peti odstavek predloga določa, da enotna kontaktna točka vsake tri mesece predloži zbirno poročilo o prejetih priglasitvah na ENISA.

Šesti odstavek predloga ureja področje ozaveščanja javnosti kadar je potrebno za preprečitev pomembnega incidenta ali obravnavo pomembnega incidenta, ki je v teku, ali kadar je razkritje pomembnega incidenta kako drugače v javnem interesu.

Sedmi odstavek predloga določa postopek, ki ga izvede PNO, ko je preko enotne kontaktne točke obveščen o pomembnem čezmejnem ali medsektorsko pomembnem incidentu, ki ima vpliv tudi v Republiki Sloveniji.

Osmi odstavek predloga določa, da mora PNO zagotoviti pristojnim organom iz zakona, ki ureja kritično infrastrukturo, informacije o pomembnih incidentih, incidentih, kibernetskih grožnjah in skorajšnjih incidentih, ki so jih priglasili bistveni subjekti, ki so identificirani kot kritični subjekti na podlagi predpisov, ki urejajo kritično infrastrukturo.

Deveti odstavek predloga določa, da mora pristojna skupina CSIRT o pomembnem incidentu nemudoma obvestiti PNO, ki vodi seznam pomembnih incidentov. S tem se prenaša tudi tretji odstavek 13. člena Direktive (EU) 2022/2555, ker je PNO hkrati enotna kontaktna točka. Pristojni nacionalni organ o incidentu, ki bi lahko imel večji medsektorski vpliv oziroma bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti Republike Slovenije, obvesti Nacionalni center za krizno upravljanje, lahko pa obvesti tudi druge pristojne organe, s katerimi sodeluje na nacionalni ravni v skladu s 17. členom tega zakona.

Deseti odstavek predloga predvideva vzpostavitev namenske digitalne platforme za priglasitev, ki jo vzpostavijo skupine CSIRT in pristojni nacionalni organ. Gre za prenos šestega odstavka 13. člena Direktive (EU) 2022/2555.

Enajsti odstavek predloga ohranja ureditev iz obstoječega zakona, ki ureja področje informacijske varnosti, ki določa, da PNO vodi (1) skupen seznam pomembnih incidentov, ki vsebuje podatke iz končnih poročil o incidentih iz tega člena in(2) seznam omrežnih in informacijskih sistemov, delov omrežja in digitalnih oziroma elektronskih komunikacijskih storitev zavezancev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

V. Ukrepi za obvladovanje tveganj in priglasitve incidentov

Poglavje vsebuje določbe glede pristojnosti in teritorialnost, zbiranja informacij za register ponudnikov storitev pri ENISA in podatkovne zbirke o registraciji domenskih imen.

K 27. členu

V tem predlogu člena gre za prenos določb 26. člena Direktive (EU) 2022/2555, ki določa pristojnost in teritorialnost.

Prvi odstavek predloga določa, da zavezanci na podlagi tega zakona spadajo v pristojnost pristojne skupine CSIRT, ki ji priglašajo incidente, če jih je ustanovila Republika Slovenija ali imajo sedež v Republiki Sloveniji. Izjemi se nanašata na (1) ponudnike javnih elektronskih komunikacijskih omrežij ali ponudnike javno dostopnih elektronskih komunikacijskih storitev šteje, da spadajo v pristojnost države članice Evropske unije, v kateri zagotavljajo svoje storitve in (2) 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 iskalnikov in platform za storitve družbenega mreženja šteje, da spadajo v pristojnost države članice, v kateri imajo glavni sedež v Evropski uniji v skladu z drugim odstavkom tega člena. Za slednje drugi odstavek predloga določa, da imajo glavni sedež v Evropski uniji v državi članici Evropske unije, kjer se sprejme večina odločitev v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. Če te države članice Evropske unije ni mogoče določiti ali če se te odločitve ne sprejemajo v Evropski uniji,

se šteje, da je glavni sedež v državi članici Evropske unije, kjer se izvajajo operacije v zvezi s kibernetsko varnostjo. Če te države članice Evropske unije ni mogoče določiti, se šteje, da je glavni sedež v državi članici, kjer ima zadevni subjekt sedež z največjim številom zaposlenih v Evropski uniji.

Tretji odstavek predloga uvaja rešitev, za subjekt, ki nima sedeža v Evropski uniji, v njej pa zagotavlja takšne storitve, določi sedež svojega predstavnika za Evropsko unijo v Republiki Sloveniji, kjer tudi zagotavlja takšne storitve, spada v pristojnost pristojnega nacionalnega organa in pristojne skupine CSIRT. Predstavnik zastopa subjekt v zvezi z obveznostmi na podlagi tega zakona.

Četrti odstavek predloga določa postopek, subjekt ni imenoval predstavnika v Evropski uniji opravlja pa storitve v Republiki Slovenije.

Peti odstavek predloga določa postopek, če PNO organ prejme zahtevek za medsebojno pomoč na podlagi 49. člena tega zakona v zvezi s subjektom iz druge alineje prvega odstavka tega člena.

K 28. členu

V tem predlogu člena gre za prenos določb 27. člena Direktive (EU) 2022/2555, ki določa register subjektov oziroma zbiranje informacij za register ponudnikov storitev pri ENISA.

Prvi odstavek predloga določa, da subjekti, ki sodijo v pristojnost PNO morajo podati informacije (1) ime subjekta; (2) ustrezni sektor, podsektor in vrsto subjekta iz Priloge I ali II, kadar je to ustrezno; (3) naslov njegovega glavnega sedeža in njegovih drugih zakonitih sedežev v Evropski uniji ali, če nima sedeža v Evropski uniji, njegovega predstavnika, imenovanega v skladu s tretjim odstavkom 27. člena tega zakona; (4) posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjekta in po potrebi njegovega zastopnika, imenovanega v skladu s tretjim odstavkom 27. člena tega zakona; (5) države članice, v katerih subjekt opravlja storitve, ter (6) bloke subjektu dodeljenih številk avtonomnih sistemov in javnih naslovov IP.

Drugi odstavek predloga določa, da morajo subjekti PNO obvestiti o vsaki spremembi informacij iz prvega odstavka.

Tretji odstavek predloga določa, da subjekti predložijo informacije PNO prek mehanizma za samoregistracijo zavezancev iz prvega odstavka 7. člena predloga zakona.

Četrti odstavek predloga določa postopek posredovanja zbranih informacij ENISI, ki vzpostavitvi in vzdržuje registra ponudnikov storitev iz prvega odstavka tega člena.

K 29. členu

V tem predlogu člena gre za prenos določb 28. člena Direktive (EU) 2022/2555, ki določa podatkovno zbirko o registraciji domenskih imen.

Prvi odstavek predloga določa, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen zaradi zagotovitve varnosti, stabilnosti in odpornosti DNS z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v posebni podatkovni zbirki, pri čemer za zbrane osebne podatke upoštevajo predpise s področja varstva osebnih podatkov.

Drugi odstavek predloga določa, da morajo podatkovna zbirke vsebovati potrebne informacije o registraciji domenskih imen, ki vsebujejo potrebne informacije za identifikacijo imetnikov domenskih imen in kontaktnih točk, ki upravljajo domenska imena v okviru vrhnjih domenskih imen, in navezavo stika z njimi.

Tretji odstavek predloga nalaga vzpostavitev politike in postopke, vključno s postopki preverjanja, ki zagotavljajo, da podatkovne zbirke iz prvega odstavka tega člena vključujejo točne in popolne informacije. Te politike in postopki morajo biti javno dostopni.

Četrti odstavek predloga določa, da subjekti po registraciji domenskega imena brez nepotrebnega odlašanja podatke o registraciji, ki niso osebni podatki, naredijo javno dostopne.

Peti odstavek določa postopek dostopa do podatkov o registraciji posameznih domenskih imen na podlagi zakonitih in ustrezno utemeljenih zahtevkov oseb, ki imajo upravičen razlog za dostop, v skladu s predpisu s področja varstva osebnih podatkov.

Šesti odstavek predloga pa uvaja varovalo pred podvajanjem zbiranja podatkov o registraciji domenskih imen.

VI. Izmenjava informacij

Poglavje vsebuje določbi glede dogovorov o izmenjavi informacij o kibernetski varnosti in prostovoljne priglasitve.

K 30. členu

V tem predlogu člena gre za prenos določb 29. člena Direktive (EU) 2022/2555, ki določa dogovore o izmenjavi informacij o kibernetski varnost. Zakonski člen obravnava izmenjavo informacij med zavezanci in pristojnimi organi v kontekstu kibernetske varnosti. Poudarja prostovoljno naravo izmenjave informacij, pravila in smernice za izmenjavo ter obveznosti zavezancev in organov.

Prostovoljna izmenjava informacij: Prvi odstavek člena omogoča zavezancem in, kadar je to ustrezno, tudi drugim subjektom, da si prostovoljno izmenjujejo informacije o kibernetski varnosti. To vključuje širok spekter informacij, kot so kibernetske grožnje, ranljivosti, tehnike odkrivanja, opozorila in priporočila za izboljšanje kibernetske varnosti.

Cilji izmenjave informacij: Izmenjava informacij je namenjena podpori preprečevanju in odkrivanju kibernetskih incidentov, zvišanju ravni kibernetske varnosti ter spodbujanju sodelovanja med javnimi in zasebnimi subjekti v boju proti kibernetskim grožnjam.

Dogovori o izmenjavi informacij: Drugi odstavek člena določa, da izmenjava informacij poteka na podlagi dogovorov med zavezanci, njihovimi dobavitelji ali ponudniki storitev. Ti dogovori upoštevajo občutljivost informacij in smernice Evropske agencije za kibernetsko varnost (ENISA).

Spodbujanje s strani pristojnega nacionalnega organa: Tretji odstavek poudarja vlogo pristojnega nacionalnega organa pri spodbujanju sklenitve dogovorov o izmenjavi informacij o kibernetski varnosti med zavezanci.

Obvestila pristojnim organom: Četrti odstavek določa, da morajo bistveni in pomembni subjekti obvestiti pristojni nacionalni organ in skupino CSIRT o svojem sodelovanju pri dogovorih o izmenjavi informacij, pa tudi o morebitnem odstopu od takšnih dogovorov.

Sodelovanje pristojnega organa: Peti odstavek omogoča pristojnemu nacionalnemu organu ali skupini CSIRT, da sodelujejo pri posamičnih dogovorih o izmenjavi informacij in določijo pogoje za informacije, ki jih dajo na voljo.

Skupaj ta člen vzpostavlja okvir za prostovoljno izmenjavo informacij med zavezanci in pristojnimi organi, ki je usmerjen v izboljšanje kibernetske varnosti, preprečevanje kibernetskih incidentov in spodbujanje sodelovanja med različnimi subjekti v kibernetskem ekosistemu.

K 31. členu

V tem predlogu člena gre za prenos določb 30. člena Direktive (EU) 2022/2555, ki določa dogovore o prostovoljni priglasitvi ustreznih informacij. V členu gre ta vpeljavo proaktivnega pristopa na področju

kibernetske varnosti Zavedati se moramo, da priglasitev kibernetskih groženj ključnega pomena. Zato se subjekte spodbuja, naj prostovoljno poročajo o kibernetskih grožnjah.

Prvi odstavek predloga zavezanim subjektom poleg obvezne priglasitve skupinam CSIRT spodbuja, da zavezanci prostovoljno priglasijo incidente, kibernetske grožnje in skorajšnje incidente in jim predložijo ustrezne informacije.

Drugi odstavek predloga omogoča, da 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 in ji predložijo ustrezne informacije.

Tretji podstavek predloga ureja, da prostovoljna priglasitev skupine CSIRT obravnavajo v skladu s postopkom iz 26. člena tega zakona. Pri prostovoljnem poročanju za priglasitveni subjekt ne veljajo nikakršne dodatne obveznosti, kar pa ne vpliva na preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

Četrti odstavek predloga nalaga pristojni skupini CSIRT, da po potrebi informacije o priglasitvah, prejetih v skladu s tem členom, kadar je potrebno, posredujejo PNO v vlogi enotne kontaktne točke, pri čemer poskrbijo za zaupnost in ustrezno varstvo informacij, ki jih je posredoval priglasitveni subjekt.

Peti odstavek predloga določa način obdelave prostovoljnih priglasitev. Pristojni skupini CSIRT pred prostovoljnimi priglasitvami lahko prednostno obravnavata obvezne priglasitve. Šesti odstavek predloga določa, da se prostovoljne priglasitve, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje storitev zavezanih subjektov in imajo zanemarljiv čezmejni vpliv, se obdela le, kadar takšna obdelava skupinama CSIRT ne pomeni nesorazmernega ali neupravičenega bremena.

Sedmi odstavek predloga določa, da se prostovoljna priglasitev ustreznih informacij iz tega člena lahko izvaja tudi po namenski digitalni platformi iz desetega odstavka 26. člena tega zakona.

VI. Vrednotenje incidenta, ocena ogroženosti in ukrepanje

Poglavje vsebuje nacionalne določbe vrednotenja incidentov in ukrepanje ter ocene ogroženosti. Gre za področje, ki je že uveljavljeno v obstoječem Zakonu o informacijski varnosti in razdelano v Nacionalnem načrtu odzivanja na kibernetske incidente. S predlaganimi določbami se kvalitetno nadgrajujejo omenjeni postopki

K 32. členu

Prvi odstavek predloga določa, da 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. Varnostne dogodke in incidente se vrednoti v naslednje stopnje s poimenovanjem C6 varnostni dogodek, C5 skorajšnji incident, C4 lažji incident, C3 težji incident, C2 težji incident in C1 kritični incident.

Drugi odstavek predloga nalaga PNO, da na podlagi podatkov in stopnje incidenta, ki mu jih sproti posredujejo skupine CSIRT, oceni ali gre hkrati tudi za kibernetski incident velikih razsežnosti ali krizo.

Tretji odstavek predloga nalaga PNO, da mora o kritičnem incidentu nemudoma obvestiti vlado in SNAV, lahko pa ju glede na presojo relevantnih okoliščin obvesti tudi o težjem incidentu kadar obstaja možnost, da preraste v kritični incident.

Četrti odstavek predloga PNO omogoča, da v primeru težjega incidenta C3, C2 ali kritičnega incidenta C1 s pisno odločbo, v nujnih primerih pa tudi ustno, določi takšne primerne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic.

Peti odstavek predloga vzpostavlja postopek, da PNO v primeru, ko nima vseh dejstev nujno potrebnih za opredelitev težjega incidenta ali kritičnega incidenta ter preprečitev nadaljnjih škodljivih posledic incidenta, lahko s pisno odločbo, v nujnih primerih pa tudi ustno od zavezanca, zahteva posredovanje dodatnih podatkov in pojasnil ter določi rok za njihovo posredovanje.

Šesti odstavek predloga nalaga, da PNO določi obseg in časovni okvir za izvedbo ukrepov.

Zoper odločbo iz četrtega in prejšnjega odstavka tega člena ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.

Sedmi odstavek predloga določa, da lahko direktor PNO lahko z namenom preprečitve nastanka krize ali njenega obvladovanja ali zaradi hitrejšega obvladovanja razmer in omejevanja nadaljnjih škodljivih posledic težjega incidenta C2 ali kritičnega incidenta C1 izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih.

Osmi odstavek predloga pa določa, da PNO o ukrepih iz četrtega in sedmega odstavka tega člena obvesti vlado in SNAV.

K 33. členu

Prvi odstavek predloga določa postopek izdelave oceno ogroženosti kibernetske varnosti v Republiki Sloveniji. PNO na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, s katerimi razpolaga ali jih pridobi, izdela oceno ogroženost, pri čemer ogroženost vrednoti kot zelo nizka, nizka, srednja, visoka ali kritična. Pri izdelavi ocene ogroženosti se upoštevajo situacijske slike stanja kibernetske varnosti v Republiki Sloveniji, EU in mednarodnem okolju; pridobljena opozorila z mednarodnim sodelovanjem; analize kibernetskih incidentov pri zavezanih subjektih; podatki, ki jih posredujejo deležniki kibernetske varnosti; zaznane ranljivosti omrežij in informacijskih sistemov in podatki pridobljeni s tehničnimi sredstvi za spremljanje stanja in prometa omrežij in informacijskih sistemov.

Drugi odstavek predloga določa, da zavezanci ne glede na oceno ogroženosti izvajajo najmanj ukrepe iz 21. člena tega zakona.

Tretji odstavek predloga določa postopek, ko je ocena ogroženosti ovrednotena kot srednja. PNO o razglasitvi obvesti zavezance in jim pri tem lahko priporoči izvedbo dodatnih ukrepov za varnost omrežij ali informacijskih sistemov. Pristojni nacionalni organ lahko o tem obvesti tudi splošno javnost prek svojih spletnih strani in sredstev javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe.

Četrti odstavek predloga določa postopek, ko je ocena ogroženosti ovrednotena kot kritična. PNO o tem nemudoma obvesti vlado in SNAV, lahko pa ju, glede na presojo relevantnih okoliščin in informacij, obvesti tudi v primeru, da je ogroženost ovrednotena kot visoka. O oceni ogroženosti visoka ali kritična, pristojni nacionalni organ obvesti zavezance, lahko pa obvesti tudi splošno javnost prek svojih spletnih strani in sredstev javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe. Pristojni nacionalni organ o preklicu ali spremembi ocene ogroženosti kritično, lahko pa tudi visoko obvesti predhodno obveščene deležnike iz tega odstavka.

Peti odstavek predloga določa seznam dodatnih ukrepov, ki jih morajo zavezanci nemudoma pričeti izvajati, ko je ocena ogroženosti visoka.

Šesti odstavek predloga določa seznam dodatnih ukrepov, ki jih morajo zavezanci nemudoma pričeti izvajati, ko je ocena ogroženosti kritična.

Sedmi odstavek predloga omogoča PNO, da zavezancu s pisno odločbo, v nujnih primerih pa tudi ustno, določi primerne in sorazmerne ukrepe, kot je potrebno za zmanjšanje ogroženosti.

Osmi odstavek predloga omejuje PNO, da se ukrepi izdani na podlagi prejšnjega odstavka določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz prejšnjega odstavka.

Deveti odstavek predloga omogoča, da direktor PNO lahko z namenom nižanja ocene ogroženosti visoka ali kritična ter posledično zaradi preprečitve nastanka krize ali njenega obvladovanja izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih, varnostno operativnih centrih oziroma skupinah CSIRT.

Deseti odstavek predloga pa določa, da PNO o ukrepih iz sedmega in devetega odstavka tega člena obvesti vlado in SNAV.

VIII. Kibernetska obramba

Poglavje vsebuje nacionalne določbe kibernetske obrambe na državni ravni, sodelovanje na področju kibernetske obrambe, pomoč na področju kibernetske obrambe ter pomoč pri kibernetski obrambi znotraj Evropske unije in na mednarodni ravni.

Gre za področje, ki je že uveljavljeno v obstoječem Zakonu o informacijski varnosti.

K 34. členu

Prvi odstavek predloga določa plasti kibernetske obrambe, drugi odstavek predloga pa namen kibernetske obrambe.

K 35. členu

S predlogom člena se postavlja sistemski okvir za kibernetsko obrambo in določa ukrepe in dejavnosti kibernetske obrambe na ravni državnih organov. Prvi odstavek predlaganega člena tako določa organe, ki izvajajo usklajene organizacijske, logično-tehnične, tehnične in administrativne ukrepe ter dejavnosti za zagotavljanje celovite kibernetske varnosti skladno s svojimi pristojnostmi. V ta namen PNO vzpostavi koordinacijsko skupino.

Drugi odstavek predloga določa, da organi, ki izvajajo kibernetsko obrambo zagotavljajo ustrezne zmogljivosti za kibernetsko obrambo na področjih, za katere so pristojni. V ta namen lahko vzpostavijo svoje varnostno operativne centre, ki morajo izpolnjevati vsaj minimalni obseg zahtev.

Tretji odstavek predloga določa, da organi stalno spremljajo stanje in odzive na dogodke v kibernetskem prostoru na področju njihovega delovanja.

Četrti odstavek predloga določa postopek vzpostavitve varnostno operativnega centra.

Peti odstavek predloga določa, da se organi za namen izvajanja kibernetske obrambe povezujejo v mednarodne povezave in z aktivnim sodelovanjem v teh povezavah ter prek drugih oblik multilateralnega in bilateralnega sodelovanja.

Šesti odstavek predloga določa obveznost tedenskega in letnega poročanja varnostno operativnih centrov PNO.

Sedmi odstavek predloga določa , da PNO osebam iz tretjega člena Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-1O) omogoči seznanitev z osnovami kibernetske varnosti s kibernetsko higieno.

K 36. členu

Prvi odstavek predloga določa sodelovanje na področju kibernetske obrambe, ki vključuje sklenitev sporazumov o sodelovanju, v katere se po potrebi vključi državne organe, organe lokalne samouprave, gospodarske družbe, zavode in druge organizacije.

Drugi odstavek predloga omogoča, da PNO lahko za namen izvajanja kibernetske obrambe k sodelovanju povabi tudi državljane in državljanke (v nadaljnjem besedilu prostovoljci).

Tretji odstavek predloga določa postopek izbora prostovoljcev in vodenje seznamov.

Četrti odstavek predloga določa pogodbeno razmerja med PNO in prostovoljcem.

Peti odstavek predloga omogoča oblikovanje operativnih skupin za kibernetsko obrambo. Šesti odstavek pa daje pristojnost direktorju PNO, da imenuje vodjo in namestnika posamezne operativne skupine in določa, da administrativno-tehnične pogoje za delovanje operativnih skupin iz prejšnjega (to je petega) odstavka zagotovi pristojni nacionalni organ.

K 37. členu

Predlagani člen omogoča PNO, da lahko nudi zavezancem dodatno pomoč na področju kibernetske obrambe v primeru kibernetskih groženj in incidentov, o katerih pristojni nacionalni organ obvešča vlado in SNAV v skladu s tem zakonom, kot tudi v primeru kibernetskih incidentov velikih razsežnosti ali kriz. Nudenje dodatne pomoči v vsakem posamičnem primeru odobri direktor PNO, pri čemer upošteva vidike nujnosti obvladovanja stanja ali prej opisanih dogodkov, razpoložljivosti operativnih skupin in drugih zmogljivosti za izvajanje kibernetske obrambe ter aktualno oceno kibernetske varnosti v državi.

K 38. členu

Republika Slovenija lahko zaprosi za pomoč pri izvajanju kibernetske obrambe druge države članice Evropske unije oziroma ustrezne institucije, organe, urade in agencij Evropske unije. Republika Slovenija lahko prej navedenim subjektom tudi nudi pomoč pri izvajanju kibernetske obrambe. O prejemu zaprosila pristojnih institucij ali organov druge države ali držav članic Evropske unije za nudenje pomoči pri kibernetski obrambi, pristojni nacionalni organ obvesti SNAV, ki o predlogu odziva na takšno zaprosilo oblikuje stališče in ga posreduje v odločanje vladi.

K 39. členu

Republika Slovenija lahko zaprosi za pomoč pri izvajanju kibernetske obrambe tudi tretje države ali mednarodne organizacije, s katerimi ima sklenjene mednarodne sporazume. Republika Slovenija lahko prej navedenim subjektom tudi nudi pomoč pri izvajanju kibernetske obrambe. Za nudenje in prejem pomoči se smiselno uporabljajo določbe 38. člena. Republika Slovenija lahko sodeluje v skupnih enotah za kibernetsko obrambo, ki jih vzpostavijo mednarodne organizacije, katerih članica je. Odločitev o takšnem sodelovanju, na predlog SNAV, sprejme vlada.

K 40. členu

Ta člen obravnava delo uslužbencev državnih organov, ki izvajajo kibernetsko obrambo, v manj ugodnih delovnih časih, kadar je to potrebno za izvajanje z zakonom določenih nalog.

Obveznost dela v manj ugodnem delovnem času: Prvi odstavek člena določa, da morajo uslužbenci državnih organov, ki izvajajo kibernetsko obrambo, opravljati delo tudi v manj ugodnem delovnem času, kadar je to potrebno za izvajanje z zakonom določenih nalog. To poudarja potrebo po fleksibilnosti in pripravljenosti za odzivanje na kibernetske grožnje v vseh delovnih časih.

Opredelitev dela v manj ugodnem delovnem času: Drugi odstavek člena podrobno opisuje, kaj se šteje za delo v manj ugodnem delovnem času. To vključuje delo v neenakomerno razporejenem delovnem času, delo v izmenah, delo ob sobotah, nedeljah, praznikih in drugih dela prostih dnevih, delo preko polnega delovnega časa, popoldansko in nočno delo in delo v deljenem delovnem času.

Pogoji dela v neenakomerno razporejenem delovnem času: Tretji odstavek člena pojasnjuje, da delo v neenakomerno razporejenem delovnem času oziroma v izmenah vključuje tudi delo ob sobotah, nedeljah, praznikih in drugih dela prostih dnevih ter delo v popoldanskem in nočnem času s prerazporeditvijo delovnega časa v okviru določene redne mesečne oziroma letne delovne obveznosti.

Določitev delovnih mest: Četrti odstavek člena določa, da se delovna mesta, na katerih poteka delo v skladu s prejšnjim odstavkom, določijo v aktu o organizaciji in sistemizaciji.

Izjeme v varnostnih razmerah: Peti odstavek člena omogoča, da se v primeru varnostnih razmer ali nujnosti opravila, ki jih ni mogoče odlagati, odredi tudi druge oblike dela, kot so določene v drugem odstavku tega člena.

Pooblastila predstojnika: Šesti odstavek člena določa, da predstojnik državnega organa določi primere, v katerih je dovoljeno odrediti delo iz prejšnjega odstavka, ter osebe, ki ga lahko odredijo.

Skupaj ta člen vzpostavlja okvir za zagotavljanje neprekinjenega delovanja kibernetske obrambe v Republiki Sloveniji, ki je ključnega pomena za varnost in obrambo države pred kibernetskimi grožnjami. Uslužbenci državnih organov, ki izvajajo kibernetsko obrambo, so tako zavezani k opravljanju dela v manj ugodnih delovnih časih, kadar je to potrebno za učinkovito obvladovanje kibernetskih tveganj in groženj.

IX. Nadzor

V tem poglavju predlog zakona ureja področje nadzora, in sicer pristojnosti za nadzor, postopek, pravna sredstva ter upravne ukrepe inšpekcijskega organa. Zaradi različne narave obeh kategorij zavezancev (bistveni in pomembni subjekti) je, upoštevaje Direktivo (EU) 2022/2555 (32. in 33. člen), za vsakega od njih predvidena specifičen postopek in dovoljen obseg nadzora. Zakon predvideva tudi, da so inšpektorji za informacijsko varnost PNO (v nadaljnjem besedilu: inšpektor) pristojni tudi za nadzor nad izvajanjem določb Akta o kibernetski varnosti, ki se nanaša na evropske certifikacijske sheme ter nad izvršitvijo upravnih odločb nacionalnega certifikacijskega organa za kibernetsko varnost.

K 41. členu

Predlagani člen prenaša določbe 31. člena Direktive (EU) 2022/2555, ki določa splošne vidike, povezane z nadzorom in izvrševanjem.

Prvi odstavek določa pristojnost za nadzor nad izvajanjem določb tega zakona, na njegovi podlagi sprejetih predpisov in upravnih odločb na podlagi tega zakona. Predlagano je, da nadzor opravljajo inšpektorji.

Drugi odstavek določa pristojnost inšpektorjev za nadzor nad evropskimi certifikacijskimi shemami iz Akta o kibernetski varnosti ter nad izvršitvijo upravnih odločb, ki jih izda URSIV kot nacionalni certifikacijski organ za kibernetsko varnost.

Tretji odstavek določa, da se za postopek nadzora po tem zakonu uporablja ZIN, razen kadar ta zakon določa drugače.

Četrti odstavek določa način, na katerega inšpektorju izvajajo nadzor in preverjajo, kako zavezanci iz tega zakona izpolnjujejo svoje obveznosti, predpisane s tem zakonom. Poleg vpogleda v podatke in

dokumentacijo smejo inšpektorju tudi neposredno vpogledati v omrežne in informacijske sisteme z namenom preverjanja pogojev in izpolnjevanja obveznosti in izvajanja ukrepov za obvladovanje tveganj kibernetske varnosti. Nadzor in preverjanje se lahko izvede na podlagi zahtev pristojnih organov iz tega zakona, pregleda poročil o izvedenih revizijah, na podlagi izvedenega varnostnega pregleda omrežja in informacijskih sistemov ali pregledom druge dokumentacije.

Peti odstavek zavezancem nalaga dolžnost sodelovanja z inšpektorji pri izvedbi inšpekcijskega nadzora na način, da morajo inšpektorjem omogočiti popoln in takojšen dostop do sistemov, območij, objektov in prostorov, ki so predmet nadzora ali so povezani z njim.

Šesti odstavek določa, da je zoper odločbe, izdane v postopkih nadzora po tem zakonu, dovoljen upravni spor. ZUP namreč v 13. členu določa, da je mogoče samo z zakonom predpisati, da v upravni zadevi pritožba ni dovoljena, hkrati pa izrecno določa, da pritožba ni dovoljena, če je za odločanje na prvi stopnji pristojen predstavniški organ ali vlada. Kot pristojno sodišče za upravni spor se določi Upravno sodišče RS, upravni spori zoper odločbe v postopkih po tem zakonu pa se morajo obravnavati nujno in prednostno.

Sedmi odstavek določa način, na katerega lahko zavezanec zaprosi za podaljšanje roka za odpravo nepravilnosti in pomanjkljivosti. Izvedba odrejenih ukrepov je običajno povezana s potrebnim časom, viri in roki za izvedbo potrebnih naročil, ki jih ni mogoče vnaprej točno predvideti. Ker se določen rok za izvedbo odrejenih ukrepov inšpektorja šteje za materialni rok, tega ni možno podaljšati na podlagi 99. člena ZUP in je za to potrebna pravna podlaga v področnem predpisu.

Osmi odstavek določa, da sme inšpektor poleg ukrepov iz ZIN uporabiti tudi ukrepe iz tega zakona. Ker so inšpektorji pristojni tudi za nadzor nad evropskimi certifikacijskimi shemami iz Akta o kibernetski varnosti ter nad izvršitvijo upravnih odločb, ki jih izda URSIV kot nacionalni certifikacijski organ za kibernetsko varnost, ta odstavek določa tudi, da smejo inšpektorji odrediti tudi ukrepe iz Akta o kibernetski varnosti.

Deveti odstavek inšpektorjem nalaga, da morajo odrejene ukrepe utemeljiti, pred sprejetjem ukrepov pa daje zavezancem možnost, da se do njih opredelijo in nanje podajo pripombe. Izjema od tega načela je dovoljena, kadar je treba sprejeti nujne ukrepe za preprečitev incidenta ali odziv nanj.

Deseti odstavek določa način razvrščanja nadzorov zavezancev in inšpektorju nalaga, da mora pri tem upoštevati pristop, ki temelji na tveganjih. Večje, kot je tveganje in hujše kot so posledice, ki lahko nastanejo, višje je zavezanec pri razvrstitvi.

K 42. členu

V tem predlogu člena gre za prenos določb prvega, drugega, tretjega, devetega in desetega odstavka 32. člena Direktive (EU) 2022/2555, ki določa nadzor in izvršilne ukrepe v zvezi z bistvenimi subjekti. Ta člen jasno opredeljuje pooblastila inšpektorja ter pravice in obveznosti bistvenih subjektov, s čimer prispeva k učinkovitemu nadzoru nad varnostjo informacijskih in kibernetskih sistemov.

Prvi odstavek predloga določa pooblastila, ki jih ima inšpektor pri izvajanju nadzora v zvezi z bistvenimi subjekti.

Drugi odstavek predloga določa ukrepe za odpravo pomanjkljivosti ali izpolnitev zahtev inšpektorja, ko ugotovi, da izrečeni ukrepi niso bili učinkoviti.

Tretji odstavek predloga mogoča začasni preklic ali prepoved, dokler zadevni bistveni subjekt ne sprejme potrebnih ukrepov za odpravo pomanjkljivosti ali ne izpolni zahtev inšpektorja, zaradi katerih je bil tak ukrep uporabljen.

Četrti odstavek predloga določa izjemo, da se ukrepi iz drugega odstavka tega člena ne uporabljajo za subjekte javne uprave, za katere velja ta zakon.

Peti odstavek predloga določa, da inšpektor pri sprejemanju ukrepov iz tega člena spoštuje postopkovne pravice bistvenega subjekta v postopku nadzora in upošteva okoliščine vsakega posameznega primera.

Šesti odstavek določa, da morajo biti naloženi ukrepi učinkoviti, sorazmerni in odvračilni

Sedmi in osmi odstavek predloga določata način izvedbe ciljno usmerjene revizije varnosti ter stroške le-te.

Deveti odstavek predloga nalaga inšpektorju, da navede namen zahteve in opredeli zahtevane informacije.

Deseti odstavek predloga določa, da inšpektor obvesti pristojno inšpekcijo za področje kritične infrastrukture, kadar izvaja nadzor nad subjektom, ki je na podlagi zakona, ki ureja kritično infrastrukturo določen kot kritičen.

Enajsti odstavek predloga določa, inšpektor sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554.

Dvanajsti odstavek predloga določa postopek upravne izvršbe izvršljivih odločb, ki jih je izdal inšpektor v postopku nadzora bistvenih subjektov.

Trinajsti odstavek predloga določa, da se ukrep iz osmega odstavka ne uporabljajo za pravne osebe javnega prava. Za njihove odgovorne osebe pa se za prisilne ukrepe z izrekanjem denarnih kazni uporabljajo določbe zakona o splošnem upravnem postopku.

Štirinajsti odstavek predloga določa kdo je odgovorna oseba za skladnost delovanja bistvenega subjekta

K 43. členu

V tem predlogu člena gre za prenos določb prvega, drugega, tretjega, četrtega, petega in šestega odstavka 33. člena Direktive (EU) 2022/2555, ki določa nadzor in izvršilne ukrepe v zvezi s pomembnimi subjekti. Ta člen jasno opredeljuje pooblastila inšpektorja ter pravice in obveznosti pomembnih subjektov, s čimer prispeva k učinkovitemu nadzoru nad varnostjo informacijskih in kibernetskih sistemov.

Prvi odstavek predloga določa kdaj se izvede inšpekcijski nadzor.

Drugi odstavek predloga določa pooblastila, ki jih ima inšpektor pri izvajanju nadzora v zvezi s pomembnimi subjekti.

Tretji odstavek predloga določa ukrepe za odpravo pomanjkljivosti ali izpolnitev zahtev inšpektorja, ko ugotovi, da izrečeni ukrepi niso bili učinkoviti.

Četrti in peti odstavek predloga določa postopek ciljno usmerjene revizije skladnosti ter stroške

Šesti odstavek predloga določa kdo je odgovorna oseba za zagotavljanje skladnosti delovanja pomembnega subjekta.

Sedmi odstavek predloga določa postopek upravne izvršbe izvršljivih določb, ki jih je izdal inšpektor v postopku nadzora pomembnih subjektov.

Osmi odstavek predloga določa, da se ukrep iz sedmega odstavka ne uporabljajo za pravne osebe javnega prava. Za njihove odgovorne osebe pa se za prisilne ukrepe z izrekanjem denarnih kazni uporabljajo določbe zakona o splošnem upravnem postopku.

Deveti odstavek predloga določa, inšpektor sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554.

K 44. členu

Ta člen določa postopek inšpekcijskega nadzora nad subjekti v skladu z Uredbo (EU) 2019/881 o kibernetski varnosti in omogoča inšpektorju učinkovit nadzor nad subjekti glede skladnosti z Uredbo (EU) 2019/881 ter zagotavlja, da subjekti izpolnjujejo zahteve glede kibernetske varnosti v skladu z evropsko zakonodajo.

Prvi odstavek predloga določa izvedbo inšpekcijskega nadzora. Inšpekcijski nadzor se izvede, če inšpektor prejme dokaze, indice ali informacije, da subjekt ne izpolnjuje zahtev iz Uredbe (EU) 2019/881 ali evropske certifikacijske sheme.

Drugi odstavek predloga določa pooblastila inšpektorja. Poleg pooblastil, ki jih določa zakon o inšpekcijskem nadzoru, inšpektorju omogoča opravljanje inšpekcijskega pregleda na kraju samem ali na daljavo, v sodelovanju s strokovnjaki; odreditev ciljno usmerjene revizije skladnosti z Uredbo (EU) 2019/881, ki jo izvede preizkušeni revizor informacijskih sistemov; odreditev ustreznih ukrepov za zagotovitev skladnosti s predpisi in predlog nacionalnemu certifikacijskemu organu za kibernetsko varnost odvzema evropskega certifikata kibernetske varnosti v primeru neskladnosti s to uredbo ali evropsko certifikacijsko shemo.

Tretji odstavek predloga določa poročilo o reviziji skladnosti. Poročilo o izvedeni ciljno usmerjeni reviziji skladnosti je na voljo inšpektorju.

Četrti odstavek predloga določa kritje stroškov. Stroške ciljno usmerjene revizije skladnosti krije subjekt, ki je predmet nadzora.

Peti odstavek predloga določa opredelitev in namen zahteve inšpektorja. Inšpektor pri izvajanju svojih pooblastil navede namen zahteve in opredeli zahtevane informacije ter določi obseg ciljno usmerjene revizije skladnosti.

K 45 členu

Prvi odstavek predloga določa, da 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.

Drugi odstavek določa časovni okvir izvajanja ocene skladnosti bistvenih subjektov med tem ko morajo pomembni subjekti po tretjem odstavku izvesti oceno skladnosti na zahtevo inšpektorja ali v primeru pojava pomembnega incidenta.

Četrti odstavek določa, da poročilo o izvedeni oceni skladnosti pripravi revizor.

Peti in šesti odstavek predloga opredeljujeta dostop inšpektorja do poročila.

Stroške izvedbe ocene skladnosti določa sedmi odstavek predloga.

K 46. členu

V skladu s prvim odstavkom predloga pomembni subjekti opravijo samoocene skladnosti enkrat na dve leti. 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. Pomembni subjekti so dolžni izjavo iz prejšnjega odstavka tega člena brez odlašanja predložiti inšpektorju, v osmih dneh od njene sestave. Stroške izvajanja samoocene skladnosti nosijo pomembni subjekti.

K 47. členu

Predlog člena določa postopek določitve preizkušenega revizorja za izvedbo revizije varnosti, ki jo zahteva inšpektor po tem zakonu.

K 48. členu

V tem predlogu člena gre za prenos določb 35. člena Direktive (EU) 2022/2555, ki opredeljuje kršitve, ki pomenijo kršitev varstva osebnih podatkov.

Prvi odstavek predloga določa da inšpektor o obravnavi zadev iz prvega odstavka 40. člena tega zakona, katerih posledica je kršitev varstva osebnih podatkov, obvešča Informacijskega pooblaščenca brez nepotrebnega odlašanja.

Drugi odstavek predloga opredeljuje postopek, kadar Informacijski pooblaščenec zaradi kršitve določbe točka (i) drugega odstavka 58. člena Uredbe (EU) 2016/679 naloži globo na podlagi zakona, ki ureja varstvo osebnih podatkov.

Tretji odstavek predloga pa določa postopke kadar ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679, sedež v drugi državi članici.

K 49. členu

V tem predlogu člena gre za prenos določb 37. člena Direktive (EU) 2022/2555, ki opredeljuje medsebojna pomoč.

Prvi odstavek predloga opredeljuje področje, kadar bistveni ali pomembni subjekt spada v pristojnost pristojnega nacionalnega organa v skladu s 27. členom tega zakona, vendar opravlja storitve v več kot eni državi članici Evropske unije ali opravlja storitve v eni ali več državah članicah Evropske unije, njegovi omrežni in informacijski sistemi pa se nahajajo v drugi državi članici Evropske unije oziroma v več kot eni državi članici Evropske unije, inšpektor lahko izvaja inšpekcijski nadzor nad temi subjekti v sodelovanju s pristojnimi organi nadzora zadevnih drugih držav članic Evropske unije. Inšpektor in pristojni organi nadzora drugih držav članic Evropske unije si medsebojno pomagajo pri izvajanju takega nadzora.

Drugi in tretji odstavek predloga opredeljujeta postopek izvajanja medsebojne pomoči iz prejšnjega odstavka, ki ga izvaja inšpektor preko enotne kontaktne točke ter vsebino zahteve za medsebojno pomoč.

Četrti odstavek predloga opredeljuje postopke inšpektorja, ki jih mora izvesti ob prejemu zahtevka za medsebojno pomoč oziroma ob zavrnitvi le-tega. Po predlaganem petem odstavku se pred zavrnitvijo zahteve za medsebojno pomoč e inšpektor posvetuje z drugimi pristojnim organi nadzora držav članic Evropske unije, ki so tudi pristojne za obravnavo nadzora v konkretnem primeru. Šesti odstavek predloga pa opredeljuje možnost skupnih inšpekcijskih nadzorov.

K 50. členu

V tem predlogu člena gre za način prenosa določb 34. člena Direktive (EU) 2022/2555, ki sicer določa splošne pogoje za naložitev upravnih glob bistvenim in pomembnim subjektom, pri čemer se cilj tega čelna navedene direktive zagotavlja preko prekrškovnih sankcij.

Prvi odstavek predloga poleg splošnih pravil za odmero sankcije iz zakona, ki ureja prekrške, pri odločanju o višini izrečene globe za kršitve določb 20., 21., 25. ali 26. člena predlaganega a zakona s strani bistvenih subjektov in pomembnih subjektov upošteva tudi letni promet oziroma letna bilančna vsota bistvenega ali pomembnega subjekta v predhodnem poslovnem letu.

Drugi odstavek predloga določa mejne vrednosti za bistvene subjekte.

Tretji odstavek predloga določa mejne vrednosti za pomembne subjekte.

Četrti odstavek določa, da se pri določanju o naložitvi in višini višine globe iz tega člena upoštevajo okoliščine posameznega primera in vsaj elementi določeni v pravem odstavku 42. člena predlaganega zakona.

K 51. členu

Po predlogu člena se sme za prekrške iz predlaganega zakona v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom.

K 52. členu

Po predlogu člena se do sprememb določb o višinah in razponih glob, ki jih določa zakon, ki ureja prekrške, višine in razponi glob, določeni v 50. členu predlaganega a zakona, uporabljajo ne glede na določbe zakona, ki ureja prekrške.

X. Kazenske določbe

V tem poglavju predloga zakona so predpisane kazni za kršitev njegovih določb. Poglavje obsega prekrške bistvenih subjektov, prekrške pomembnih subjektov in prekrške upravljavca centralnega informacijsko-komunikacijskega sistema in ob kršitvah Uredbe (EU) 2019/881).

K 53. členu

Predlog člena določa globe, ki se lahko izrečejo bistvenim subjektom.

K 54. členu

Predlog člena določa globe, ki se lahko izrečejo pomembnim subjektom.

K 55. členu

Predlog člena določa globe, ki se lahko izrečejo upravljavcu centralnega informacijsko-komunikacijskega sistema.

K 56. členu

Predlog člena določa globe, ki se lahko izrečejo ob kršitvah Uredbe (EU) 2019/881).

XI. Prehodne določbe

Predlagano poglavje vsebuje določbe glede vzpostavitve samoregistracije, seznamov in obveščanja, prehodnega obdobja za sprejem ukrepov za obvladovanje tveganj in uskladitve obstoječe podatkovne zbirke o registraciji domenskih imen, izdaje podzakonskih predpisov in strategije, prenehanja veljavnosti in podaljšanja uporabe predpisov, sprememb in dopolnitev zakona, ki ureja elektronske

komunikacije, dopolnitve zakona, ki ureja prekrške, spremembe zakona, ki ureja varstvo osebnih podatkov ter dokončanja postopkov, začetih pred uporabo tega zakona.

K 57. členu

V predlaganem členu se urejajo roki za vzpostavitev mehanizma za samoregistracijo zavezancev, za vzpostavitev seznama zavezancev in za obveščanje Evropske komisije s strani PNO. Postavljen je tudi rok za seznanitev PNO z identiteto subjektov, ki so na podlagi po učinku enakovrednih obveznosti druge sektorske zakonodaje glede ukrepov in poročanja o incidentih izvzeti iz zadevnih obveznosti po predlaganem zakonu, pri premer so za takšno seznanitev zadolženi pristojni organi druge sektorske zakonodaje

Določa se tudi rok do katerega PNO obvesti Evropsko komisijo o določitvi enotne kontaktne točke, o določitvi organa za obvladovanje kibernetskih kriz, o identiteti skupin CSIRT.

PNO vzpostavi digitalno platformo za medsebojno izmenjava informacij o relevantnih incidentih, kibernetskih grožnjah in skorajšnjih incidentih v enem letu od uveljavitve tega zakona.
Skupine CSIRT in PNO vzpostavijo namensko digitalno platformo iz desetega odstavka 26. člena v enem letu od uveljavitve tega zakona.

Subjekti iz prvega odstavka 28. člena tega zakona o informacijah iz navedene določbe prvič obvestijo pristojni nacionalni organ do 17. januarja 2025, ki te informacije brez nepotrebnega odlašanja prvič posreduje ENISA na način iz četrtega odstavka 28. člena tega zakona.

Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen vzpostavijo politike in postopke iz tretjega in petega odstavka 29. člena v šestih mesecih od uveljavitve tega zakona.

Organi iz prvega odstavka 35. člena tega zakona pristojni nacionalni organ obvestijo o obstoječih varnostno operativnih centrih, ki izpolnjujejo zahteve iz drugega odstavka 35. člena v tridesetih dneh od uveljavitve tega zakona.

Organi iz prvega odstavka 35. člena tega zakona pristojni nacionalni organ obvestijo o obstoječih varnostno operativnih centrih, ki ne izpolnjujejo zahtev iz drugega odstavka 35. člena v tridesetih dneh od uveljavitve tega zakona, zagotovijo izpolnjevanje le-teh v enem letu od uveljavitve zakona.

Pristojni nacionalni organ v teh mesecih od sprejetja nacionalnega načrt odzivanja iz četrtega odstavka 58. člena tega zakona predloži Evropski komisiji in mreži EU-CyCLONe ustrezne informacije.

K 58. členu

Po predlogu tega člena v roku dvanajstih mesecev od uveljavitve tega zakona bistveni in pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost iz 20. in 21. člena tega zakona. Ob tem je za izvajalce bistvenih storitev, ki so bili določeni pred 16. januarjem 2023 ter za operaterje po ZEKom-2 ta rok šest mesecev.

K 59. členu

Predlaga se, da v roku osemnajstih mesecev od uveljavitve tega zakona registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen uskladijo obstoječe podatkovne zbirke o registraciji domenskih imen z drugim in četrtim odstavkom 29. člena tega zakona za registracije, ki so bile izvedene do uveljavitve tega zakona.

K 60. členu

Predlog člena določa roke za izdajo obveznih podzakonskih predpisov po tem zakonu in za sprejetje Strategije kibernetske varnost v skladu z določbami tega zakona. Do sprejetja te strategije se

uporablja Strategija kibernetske varnosti Republike Slovenije, ki jo je sprejela vlada dne 25. februarja 2016 s sklepom št. 38100-12/2015/5.

K 61. členu

Predlog člen določa prenehanje veljavnosti predpisov ter smiselno uporabo le-teh do izdaje podzakonskih predpisov sprejetih na podlagi tega zakona.

K 62. členu

S predlogom člena se spremenijo in dopolnijo določbe Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2).

Pojasnjujemo razloge za predlagani poseg v ZEKom-2. Namreč, sedaj veljavni ZInfV v tretjem odstavku 2. člena določa: »Ta zakon se ne uporablja za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve (operaterji), za katere veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev iz zakona, ki ureja elektronske komunikacije, ter za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (UL L št. 257 z dne 28. 8. 2014, str. 73).« S to določbo ZInfV se je takrat sledilo določbi tretjega odstavka 1. člena Direktive 2016/1148/ES ter njeni Uvodni izjavi št. 7. Medtem, ko so bile takšne posebne določbe Uredbe (EU) št. 910/2014 neposredno uporabljive, pa je takratni Zakon o elektronskih komunikacijah (Uradni list RS, št. št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17; v nadaljnjem besedilu: ZEKom-1) v slovenski pravni red prenašal takšne posebne zahteve za operaterje iz določb členov 13a in 13b takratne Direktive 2002/21/ES[10]. Medtem je sicer zadnja omenjena direktiva, skupaj s pretežno večino takratnih direktiv s področja elektronskih komunikacij, prenehala veljati v skladu z novo Direktivo (EU) 2018/1972[11], ki pa je ponovno vsebovala takšne posebne obveznosti za operaterje elektronskih komunikacij in sicer njenih v členih 40 in 41. Direktiva (EU) 2018/1972 je bila prenesena v slovenski pravni red z novim Zakonom elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2), ki v poglavju VIII. Varnost omrežij in storitev ter delovanje v stanjih ogroženosti ureja prenos določb 40. in 41. člena Direktiva (EU) 2018/1972, vsebuje pa tudi nacionalne sektorsko specifične določbe. Nekatere postopkovne in nadzorne določbe so bile dodane tudi zaradi približevanja ureditve ZEKom-2 sistemski ureditvi področja informacijske oziroma kibernetske varnosti po ZInfV in sicer z določitvijo nekaterih nalog v ZEKom-2 tudi za pristojni nacionalni organ iz ZInfV in njegovih inšpektorjev.

Direktiva (EU) 2022/2555, ki jo v slovenski pravni red prenašamo s predlaganim zakonom, z njenim 42. členom posega v neposredno uporabljivo Uredbo (EU) št. 910/2024 tako, da črta 19. člen navedene uredbe z učinkom od 18. 10. 2024. Z členom 43 pa Direktiva (EU) 2022/2555 posega v Direktivo (EU) 2018/1972, ki je bila v slovenski pravni red prenesena z ZEKom-2 tako, v njej črta člena 40 in 41, prav tako z učinkom od 18. oktobra 2024. Pri tem je treba še dodati, da za razliko od ZInfV in direktive, ki se je z njim prenesla v slovenski pravni red, predlagani ZInfV-1 obe prej navedeni področji urejanja oziroma subjektov, ki v tem sektorju delujejo, ne izključuje več iz področja uporabe predlaganega zakona. To je razvidno iz 3. člena (področje uporabe) predlaganega zakona in njegove pripadajoče Priloge I, ki povzemat Prilogo I Direktive (EU) 2022/2555. Pod Prilogo I predlaganega

[10] Direktiva evropskega parlamenta in sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva) (UL L 108, z dne 24. 4. 2002, str. 33) (v nadaljnjem besedilu: Direktiva 2002/21/ES

[11] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (UL L št. 321 z dne 17. 12. 2018, str. 36) (v nadaljnjem besedilu: Direktiva 2018/1972/EU).

zakona (Visoko kritični sektorji) spadajo namreč tako ponudniki storitev zaupanja, kot tudi ponudniki javnih komunikacijskih omrežij in ponudniki javno dostopnih elektronskih komunikacijskih storitev, saj spadajo med vrste subjektov, saj sodijo v (visoko kritični) Sektor »8. Digitalna infrastruktura« omenjene Priloge I. Prav tako so te kategorije sedaj izrecno navedene tudi med zavezanci iz 6. člena predlaganega zakona.

Iz zgoraj opisanih razlogov je treba s predlaganim zakonom poseči v ZEKom-2, ki je Direktivo (EU) 2018/1972 prenesel v slovenski pravni red in sicer iz razloga, da ne bi prišlo do medsebojen neusklajenosti obeh zakonov, da se prepreči nepotrebno podvajanje urejanja zadevnih obveznosti zavezancev, ki bodo po novem urejene z ZInfV in zagotovi skladnosti z EU pravnim redom. Ob tem dodajamo, da so predlagani posegi v ZEKom-2 predvsem tisti, ki so nujni za medsebojno usklajenost obeh zakonov. Sektorsko specifične dodatne rešitve oziroma ukrepi v ZEKom-2 glede varnosti in celovitosti omrežij in storitev, ki jih predlagani zakon ne ureja (kot tudi ne ureja takšnih rešitev oziroma ukrepov za ostale sektorje), torej ostajajo v ZEKom-2 oziroma so bili, kjer smo to ocenili za potrebno, le minimalno spremenjeni oziroma dopolnjeni z vidika jasnosti in ob upoštevanju razvoja stanja varnostnih tveganj v praksi.

Posledično po prvem odstavku predlaganega člena z dnem uveljavitve predlaganega zakona prenehajo veljati določbe 118. (obveznost obveščanja in poročanja o varnostnih incidentih), 119. (vrednotenje varnostnega incidenta), 120. (ukrepanje v primeru težjega in kritičnega incidenta ali kibernetskega napada), 121. (stanje povečane ogroženosti in ukrepanje), 122. (obveščanje javnosti o sprejetih ukrepih) in 123. člena (revizija varnosti) poglavja VIII. Varnost omrežij in storitev ter delovanje v stanjih ogroženosti iz ZEKom- 2. Gre namreč za vsebine, ki jih v skladu z Direktivo (EU) 2022/2555 na enak način za v predlog zakona zajete sektorje horizontalno ureja predlagani zakon ob upoštevanju, da je Direktiva (EU) 2022/2555 direktiva minimalne harmonizacije.

Predlagani člen pa v drugem odstavku posega v tam naštete določbe ZEKom-2, ki jih treba ohraniti, vendar ob spremembah besedila glede na uskladitev s predlogom tega zakona in upoštevanja pomena njihovega sektorsko specifičnega urejanja v ZEKom-2.

Posledično se 115. člen (varnost omrežij in storitev) ZEKom-2 ohranja vendar s spremenjenim besedilom, ki operaterje glede sprejema ustreznih in sorazmerni tehničnih ter organizacijskih ukrepov za ustrezno obvladovanje tveganja za varnost omrežij in storitev, vključno s pripadajočimi informacijskimi sistemi, napotuje na predlagani zakona (zakon, ki ureja informacijsko varnost). Hkrati pa se jasno in izrecno dopušča tudi dodatno sektorsko specifično urejanje s splošnim aktom Agencije za komunikacijska omrežja in storitve, Republike Slovenije (v nadaljnjem besedilu: AKOS), če so zaradi zagotovitve višje ravni kibernetske varnosti, ob upoštevanju varnostnih tveganj, potrebni tudi sektorsko specifični ukrepi za operaterje. AKOS v tem primeru namreč lahko izda splošni akt, s katerim predpiše posebne tehnične usmeritve ter tehnične in organizacijske ukrepe, pri čemer upošteva tudi dokumente ali tehnična priporočila ENISA ter smernice Evropske komisije. Pri sprejemu takšnega splošnega akta pa AKOS sodeluje z organom, pristojnim za informacijsko varnost.

Določbe 116. člena (dodatne varnostne zahteve) ZEKom-2 se ohranjajo, saj gre za je sektorsko specifično urejanje dodatnih varnostnih zahtev za ožjo skupino operaterjev. Vanj se posega le zaradi uskladitve znotraj ZEKom-2 glede na predlagano spremembo 115. člena istega zakona, čemur se zato prilagaja sklic na ta člen v prvem stavku četrtega odstavka 116. člena ZEKom-2. Tudi predlagana sprememba v četrtem odstavku 124. člena ZEKom-2 je posledica predlaganih sprememb 115. člena navedenega zakona in je zato treba v četrtem odstavku 124. člen ZEKom-2 uporabo dosedanjega petega odstavka 115. člena navedenega zakona nadomestiti z ustrezno vsebino, ki je 115. členu ni več. Poseg v 128. člen (nadzor) je potreben zaradi predlaganega črtanja 21. in 22. člena ZEKom-2, hkrati pa se izrecno vključuje tudi nadzor izvajanja odločbe iz prvega odstavka 117. člena ZEKom-2, ki je v ZEKom-2 izpadel.

Nadalje se predlaganim spremembam ZEKom-2 prilagajajo še določbe poglavja XV. NADZOR in sicer s predlaganimi spremembami členov 287, 288, 289 ZEKom-2 ter določbe poglavja XVII. KAZENSKE DOLOČBE in sicer v členih 298 (prekrški) in 299 (prekrški) ZEKom-2.

Tretji odstavek predlaganega člena pa določa, da z dnem uveljavitve tega zakona prenehata veljati splošna akta izdana na podlagi sedmega odstavka 115. in iz drugega odstavka 118. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O), ki se smiselno uporabljata do pričetka uporabe podzakonskih aktov izdanih na podlagi predlaganega zakona.

K 63. členu

Predlog člena ureja poseg v Zakonu o prekrških (Uradni list RS, št. 29/11 – uradno prečiščeno besedilo, 21/13, 111/13, 74/14 – odl. US, 92/14 – odl. US, 32/16, 15/17 – odl. US, 73/19 – odl. US, 175/20 – ZIUOPDVE in 5/21 – odl. US), v katerega se ustrezno umešča informacijska varnost.

K 64. členu

Predlog člena zaradi uskladitve s tema zakonom posega v Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22).

K 65. členu

Upravni, inšpekcijski in prekrškovni postopki, ki do začetka uporabe tega zakona še niso bili pravnomočno končani, se po predlogu tega člena končajo v skladu z dosedanjimi predpisi.

XII. Končna določba

K 66. členu

V predlaganem členu je določeno, da zakon začne veljati petnajsti dan po objavi v Uradnem listu RS.

IV. BESEDILO ČLENOV, KI SE SPREMINJAJO

/

V. PREDLOG, DA SE PREDLOG ZAKONA OBRAVNAVA PO NUJNEM OZIROMA SKRAJŠANEM POSTOPKU

/

VI. PRILOGE

Bo dopolnjeno v naslednjih fazah.