EVA 2023-1544-0005

ZAKON
O INFORMACIJSKI VARNOSTI (ZInfV–1)

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.. Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu.

2. člen
(namen zakona)

(1) Namen zakona je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah.

(2) S tem zakonom se v pravni red Republike Slovenije prenaša Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 333/142, z dne 27. 12. 2022, str.80), nazadnje popravljena s Popravkom Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 239 z dne 28. 9. 2023, str. 48) (v nadaljnjem besedilu: Direktiva 2022/2555).

3. člen
(področje uporabe zakona)

(1) Ta zakon se uporablja za javne ali zasebne subjekte vrste iz Prilog I ali II tega zakona (v nadaljnjem besedilu Priloga I ali II), ki sta sestavni del tega zakona, če imajo vsaj 50 zaposlenih in letni promet oziroma 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 za povezane subjekte, v kolikor ti niso že zajeti na podlagi prejšnjih odstavkih 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 20. 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, Komisije o uporabi člena 4 (1) in (2) Direktive 2555/2022.

4. člen
(obdelava podatkov in informacij)

(1) Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev pa tudi v skladu s predpisom, ki ureja zasebnost na področju elektronskih komunikacij. Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij pomeni zakoniti interes zadevnega upravljavca podatkov.

(2) Podatki in informacije, ki se obdelujejo na podlagi tega zakona in so opredeljeni kot tajni ali kot poslovna skrivnost ali druge oblike varovanih podatkov, se obravnavajo v skladu s področnimi predpisi, ki urejajo njihovo obravnavo in varovanje. zmenjava podatkov in informacij, ki so opredeljeni kot tajni ali poslovna skrivnost mora biti za potrebe izvajanja tega zakona omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij ter zaščiti varnost in poslovni interes zadevnih subjektov.

(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.

(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 na podlagi tega zakona ne vključujejo posredovanja podatkov in informacij, katerih razkritje bi bilo v nasprotju z vitalnimi interesi Republike Slovenije na področju nacionalne varnosti, javne varnosti ali obrambe, izven Republike Slovenije.

5. člen
(pomen izrazov)

Izrazi, uporabljeni v tem zakonu, imajo naslednji pomen:

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 informacijske 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. 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.

5. ENISA pomeni Agencijo Evropske unije za varnost omrežij in informacij.

6. 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.

7. Incident pomeni dogodek, ki ogroža razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali storitev, ki jih ti omrežni in informacijski sistemi zagotavljajo ali so prek njih dostopni.

8. 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.

9. Informacijsko okolje je skupek družbenih omrežij in kibernetskega prostora, vključno z informacijami.

10. Informacijska varnost je zaščita, varovanje in obramba informacijskega okolja 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 registriran pri Slovenskem inštitutu za revizijo in vpisan v njegov seznam aktivnih preizkušenih revizorjev informacijskih sistemov.

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

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 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 v obliki dnevniškega zapisa, ki omogoča natančen pregled vseh zapisov, povezanih z vsemi dogodki in vsemi shranjenimi informacijami, od nastanka podatka ali informacije naprej do trenutnega stanja.

46. Semaforski protokol je skupek pravil in dogovorov o omejitvah v zvezi z nadaljnjim širjenjem prejetih ali deljenih informacij.

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 skupaj z vsemi zmogljivostmi in infrastrukturami za distribucijo električne energije in okoljski nadzor.

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 subjekt, ki je v Republiki Sloveniji priznan kot samostojna oseba javnega prava, razen sodstva, parlamenta ali centralne banke, 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 na področju čezmejnega gibanja oseb in pretoka blaga, storitev ali kapitala.

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. Varovan podatek pristojnega nacionalnega organa je podatek o ranljivostih ali stanju informacijskih sistemov in omrežij zavezancev, ki ni tajen ali poslovna skrivnost njegovo razkritje nepoklicanim osebam pa bi lahko povzročilo motnje pri delovanju in izvajanju nalog pristojnemu nacionalnemu organu, oziroma bi lahko škodovalo zavezancem.

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 je notranja organizacijska enota posameznih organov državne uprave, ki se odziva na incidente na področju informacijske varnosti.

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 oziroma letno bilančno vsoto vsaj 42 milijonov evrov;
2. ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost;
3. ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov;
4. subjekti javne uprave na državni ravni;
5. vsi drugi subjekti vrste iz Prilog I ali II, ki jih na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona in na predlog pristojnega nacionalnega organa določi vlada z odločbo;
6. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo;
7. subjekti, ki so bili v skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023;
8. drugi subjekti, ki niso subjekti iz točk 1 do 7 tega odstavka, ki jih vlada lahko določi kot bistvene subjekte zaradi pomembnega negativnega vpliva, ki bi ga incident pri izvajanju njihovih storitev imel za življenje in zdravje ljudi oziroma zaradi pomembnega negativnega vpliva na okolje.

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

- subjekti vrste iz Prilog I ali II in
- drugi subjekti iz 3. člena tega zakona,

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

(4) Izvajanje 8. točke drugega odstavka tega člena vlada lahko podrobneje opredeli z metodologijo za določitev zadevnih subjektov kot bistvenih.

7. člen
(samoregistracija in seznam zavezancev)

(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz prejšnjega člena tega zakona.

(2) Zavezanci iz prejšnjega člena tega zakona se morajo registrirati preko mehanizma za samoregistracijo iz prejšnjega odstavka in ob tem podati vsaj naslednje informacije o:

- imenu in naslovu, kontaktnih podatkih, matični številki ter elektronskem naslovu zavezanca za vročanje;
- dodeljenih blokih javnih naslovov IP;

- kontaktni osebi za informacijsko varnost in njenem namestniku ter njune kontaktne podatke vključno z elektronskimi naslovi in telefonskimi številkami;
- ustreznem sektorju in podsektorju iz Priloge I ali II, v katerem zavezanec izvaja vrste storitev iz teh prilog ali kategorijo zavezancev, ki niso vključeni v navedenih prilogah, so pa zavezanci na podlagi določb tretjega do sedmega odstavka 3. člena tega;
- seznamu držav članic Evropske unije, kjer opravljajo storitve, ki spadajo na področje uporabe tega zakona ter

- registriranih številkah avtonomnih sistemov in vseh domenskih imenih, ki jih zavezanec uporablja pri poslovanju."

(3) Zavezanci iz prejšnjega člena tega zakona z uporabo mehanizma za samoregistracijo nemudoma sporočijo morebitne spremembe podatkov, ki so jih predložili na podlagi prejšnjega odstavka, v vsakem primeru pa v dveh tednih od datuma spremembe.

(4) Na podlagi informacij zavezancev iz drugega in tretjega odstavka tega člena in ob upoštevanju določb drugega, tretjega oziroma četrtega odstavka prejšnjega člena tega zakona pristojni nacionalni organ vzpostavi seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Ta seznam pristojni nacionalni organ redno oziroma vsaj vsaki dve leti pregleda in po potrebi posodobi.

(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 oziroma 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, 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 ter medsektorsko sodelovanje z drugimi pristojnimi organi za kibernetsko varnost v Republiki Sloveniji skladno s področnimi predpisi.

(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, ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave in incidentov povezanih subjektov.

(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 in niso povezani subjekti.

(4) Skupini CSIRT morata izpolnjevati zahteve iz naslednjega člena ter sta pristojni za obvladovanje incidentov v skladu s postopkom določenim s tem zakonom.

(5) Skupini CSIRT izmenjujeta 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 sodelujeta z njim pri uvajanju in uporabi orodij za varno izmenjavo informacij.

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

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

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

(9) Skupini CSIRT lahko sodelujeta 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 izmenjujeta informacije z uporabo ustreznih protokolov, vključno s semaforskim protokolom, z namenom da se zagotovi uspešen, učinkovit in varen način izmenjave informacij. Skupini CSIRT si lahko izmenjujeta 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) Skupini CSIRT lahko sodelujeta 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)

Skupini CSIRT iz prvega odstavka prejšnjega člena morata 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) Skupini CSIRT iz prvega odstavka 12. člena tega zakona na področjih za katera sta pristojna skladno z drugim ali tretjim odstavkom 12. člena tega zakona izvajata 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) Skupini CSIRT iz prvega odstavka 12. člena tega zakona lahko izvajata proaktivno in nevsiljivo pregledovanje javno dostopnih omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov, za katere sta pristojna skladno z drugim ali tretjim 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) Skupini CSIRT iz prvega odstavka 12. člena tega zakona lahko pri izvajanju nalog iz prvega odstavka tega člena prednostno razvrstita 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 obravnavali.

(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) CSIRT državne uprave je za namen učinkovitega izvajanja nalog informacijske in kibernetske varnosti ter kibernetske obrambe 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.

(8) Za namen pravočasnega odzivanja na kibernetske grožnje in preprečevanja škodljivih posledic morebitnega težjega ali kritičnega incidenta ter zaradi izvajanja kibernetske obrambe je CSIRT državne uprave pooblaščen, 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.

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

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

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

(2) Za olajšanje sodelovanja iz prejšnjega odstavka skupini CSIRT spodbujata sprejetje in uporabo skupnih ali uveljavljenih praks, sistemov razvrščanja in taksonomij v zvezi s:

- postopki obvladovanja incidentov;
- obvladovanjem kriz ter
- usklajenim razkrivanjem ranljivosti na podlagi prvega odstavka 16. člena tega zakona.

(3) Skupina CSIRT, ki zazna ranljivost informacijsko-komunikacijskega sistema, mora o tem brez nepotrebnega odlašanja obvestiti skrbnika sistema.

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.

(2)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.

(3)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.

(4)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., 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.

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

(1) Bistveni in pomembni subjekti morajo sprejeti ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih ti subjekti uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve.

(2) Ukrepi iz prejšnjega odstavka morajo ob upoštevanju najsodobnejših in po potrebi ustreznih evropskih in mednarodnih standardov ter stroškov izvajanja zagotavljati raven varnosti omrežnih in informacijskih sistemov, ki ustreza obstoječim tveganjem. Pri ocenjevanju sorazmernosti teh ukrepov bistveni in pomembni subjekti ustrezno upoštevajo:

- stopnjo izpostavljenosti tveganjem,
- velikost subjekta,
- verjetnost pojava incidentov ter
- resnost morebitnih incidentov, vključno z njihovim družbenim in gospodarskim vplivom.

(3) Ukrepi iz prvega in drugega odstavka tega člena morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščititi omrežne in informacijske sisteme ter njihovo fizično okolje pred incidenti, in morajo obsegati najmanj:

1. politike o analizi tveganja in varnosti informacijskih sistemov;
2. obvladovanje incidentov;
3. neprekinjeno poslovanje, vključno z upravljanjem varnostnih kopij in vnovično vzpostavitvijo delovanja po nepredvidljivih dogodkih ter za obvladovanje kriz;
4. varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;
5. varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti;
6. politike in postopke za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost;
7. osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;
8. politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;
9. varnost človeških virov, politike nadzora dostopa in upravljanje sredstev;
10. uporaba večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je to primerno.

(4) Bistveni in pomembni subjekti pri preučevanju ustreznih ukrepov iz 4. točke prejšnjega odstavka~~,~~ morajo upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Bistveni in pomembni subjekti morajo ugotavljati tudi kateri ukrepi so ustrezni za zagotovitev varnosti dobavne verige iz 4. točke prejšnjega odstavka. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih lahko pripravi Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA.

(5) Bistveni ali pomembni subjekti v rednih časovnih obdobjih, ki jih opredeli v politiki in postopkih iz 6. točke tretjega odstavka tega člena in ob zaznanih ranljivostih, preverjajo izpolnjevanje ukrepov iz tretjega odstavka tega člena. Če pri tem ugotovijo, da ne izpolnjujejo vseh ukrepov iz tretjega odstavka tega člena ali pa so ti neustrezno izvajani, morajo brez nepotrebnega odlašanja sprejeti vse potrebne, ustrezne in sorazmerne popravne ukrepe.

(6) Ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja in ponudniki storitev zaupanja pri sprejemu ukrepov iz tretjega odstavka tega člena upoštevajo izvedbene akte Evropske komisije iz prvega pododstavka petega odstavka 21. člena Direktive 2022/2555, s katerimi ta določi tehnične in metodološke zahteve za ukrepe.

(7) Bistveni in pomembni subjekti, ki niso navedeni v prejšnjem odstavku, pri sprejemu ukrepov iz tretjega odstavka tega člena, upoštevajo morebitne izvedbene akte Evropske komisije, s katerimi ta določi tehnične in metodološke zahteve ter po potrebi sektorske zahteve za ukrepe iz drugega pododstavka petega odstavka 21. člena Direktive 2022/2555.

(8) Vlada lahko podrobneje določi način izvajanja obveznosti iz tega člena in minimalni obseg varnostnih ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, v kolikor niso zajeti v dokumentih Evropske komisije iz šestega ali prejšnjega odstavka tega člena. Pri tem vlada upošteva tudi morebitne dokumente ali tehnična priporočila ENISA ter Skupine za sodelovanje.

(9) Bistveni in pomembni subjekti ne smejo uporabljati informacijsko-komunikacijskih rešitev, ki imajo aktivno izkoriščane ranljivosti, brez dodatne izvedbe ocene tveganja in kjer je to glede na oceno tveganja primerno, ustreznih popravljalnih ukrepov, ki znižajo stopnjo tveganja na sprejemljivo raven.

(10) Skupini CSIRT zavezance obvestita o ranljivostih informacijsko-komunikacijskih rešitev, ki jih uporabljajo zavezanci, za katere sta pristojni in s katerimi sta seznanjeni, če jih štejeta za kritične, lahko pa tudi za visoko pomembne, v skladu z mednarodno sprejetimi praksami za določanje ranljivosti.

(11) 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.

21. člen
(dnevniški zapisi)

(1) Bistveni in pomembni subjekti za namen obvladovanja in preprečevanja incidentov, v skladu s politikami o analizi tveganja in varnosti informacijskih sistemov iz prve točke tretjega odstavka 20. člena tega zakona in ob upoštevanju stanja tehnike zagotovijo tudi ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja, za obdobje šestih mesecev, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov.

(2) Ohranjanje dnevniških zapisov se zagotavlja na ozemlju Republike Slovenije, razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, glede katerih se lahko zagotavlja na ozemlju Evropske unije.

(3) Dnevniški zapisi o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja iz prejšnjega odstavka morajo biti hranjeni na način, ki zagotavlja njihovo avtentičnost, celovitost in razpoložljivost v primeru incidentov.

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
(certifikacijske sheme za kibernetsko varnost)

(1) Bistveni in pomembni subjekti zaradi zagotavljanja višje ravni kibernetske varnosti z namenom zagotovitve skladnosti z nekaterimi zahtevami iz 20. člena tega zakona

prednostno uporabljajo proizvode IKT, storitve IKT in postopke IKT ter so jih razvili bistveni ali pomembni subjekti ali ki so bili kupljeni pri tretjih straneh in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi člena 49 Uredbe (EU) 2019/881.

(2) Pristojni nacionalni organ spodbuja bistvene in pomembne subjekte, da pri izvajanju ukrepov iz 20. člena tega zakona, kjer je to možno in primerno, uporabljajo kvalificirane storitve zaupanja.

(3) Bistveni in pomembni subjekti iz kategorij, ki jih lahko 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.

24. člen
(standardizacija)

(1) Bistveni in pomembni subjekti zaradi zagotovitve skladnega izvajanja ukrepov iz 20. člena tega zakona v čim večji meri uporabljajo evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov. Pri tem upoštevajo tudi nasvete in smernice ENISA.

(2) Pristojni nacionalni organ na svoji spletni strani objavlja ustrezne informacije iz prejšnjega odstavka ter osvešča zavezance k njihovi uporabi.

25. člen
(obveznost priglašanja in obveščanja)

(1) Bistveni in pomembni subjekti pristojni skupini CSIRT brez nepotrebnega odlašanja v skladu s prvim in drugim odstavkom 26. člena tega zakona priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Pri tem se incident šteje za pomembnega, če:

- je zadevnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube;
- je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

(2) Bistveni in pomembni subjekti pri priglašanju iz prejšnjega odstavka upoštevajo morebitne izvedbene akte Evropske komisije iz prvega pododstavka enajstega odstavka 23. člena Direktive 2022/2555, s 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 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 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 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 prejemnike 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 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. Kadar je ustrezno, subjekti zadevne prejemnike 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 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 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.

V. Pristojnost in registracija

27. člen
(pristojnost in teritorialnost)

(1) 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, razen v primeru, da:

- se za ponudnike javnih elektronskih komunikacijskih omrežij ali ponudnike javno dostopnih elektronskih komunikacijskih storitev šteje, da spadajo v pristojnost države članice Evropske unije, v kateri zagotavljajo svoje storitve;
- se za ponudnike storitev DNS, registre TLD imen, subjekte, ki opravljajo storitve registracije domenskih imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov, ponudnike omrežij za dostavo vsebine, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev ter ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja šteje, da spadajo v pristojnost države članice, v kateri imajo glavni sedež v 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. 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. 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 prvega 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 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, 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 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 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.

IX. Nadzor

40. člen
(splošne določbe)

(1) Za nadzor nad izvajanjem določb tega zakona, na njegovi podlagi sprejetih predpisov in nad izvršitvijo upravnih odločb, izdanih na podlagi četrtega ali petega odstavka 32. člena sedmega odstavka 33. člena tega zakona, nad izvršitvijo odredb, izdanih na podlagi sedmega odstavka 32. člena in devetega odstavka 33. člena tega zakona, so pristojni inšpektorji za informacijsko varnost pristojnega nacionalnega organa (v nadaljnjem besedilu: inšpektor).

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

(3) 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 in 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.

(4) Inšpektor lahko od zavezancev zahteva, da predložijo informacije, potrebne za oceno varnosti njihovih omrežij in informacijskih sistemov, vključno z dokumentiranimi varnostnimi pravili, dokaze o učinkovitem izvajanju varnostnih pravil ter informacije o obravnavanih kibernetskih incidentih v določenem časovnem obdobju. Kadar inšpektor zahteva takšne informacije ali dokaze, navede namen te zahteve in opredeli, katere dodatne informacije so potrebne.

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

(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 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.

(9) Inšpektor lahko poleg ukrepov, ki jih ima po zakonu, ki ureja inšpekcijski nadzor, odredi tudi ukrepe, določene s tem zakonom.

(10) Inšpektor podrobno utemelji ukrepe iz prejšnjega odstavka. 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.

41. člen
(nadzor bistvenih subjektov)

(1) Ukrepi, ki jih inšpektor naloži bistvenim subjektom v zvezi z obveznostmi iz tega zakona morajo biti učinkoviti, sorazmerni in odvračilni, pri čemer se upoštevajo okoliščine posameznega primera.

(2) Inšpektor je pri izvajanju svojih nadzornih nalog pri bistvenih subjektih pooblaščen za to, da:

1. opravi inšpekcijske preglede na kraju samem in nadzor na daljavo, vključno z naključnimi pregledi, ki jih lahko izvede skupaj z usposobljenimi strokovnjaki;
2. zahteva izvedbo redne in ciljno usmerjene revizije varnosti, ki jo izvede preizkušeni revizor informacijskih sistemov;
3. zahteva izvedbo priložnostne revizije, tudi ko je to utemeljeno zaradi pomembnega incidenta ali kršitve tega zakona s strani bistvenega subjekta;
4. opravi varnostne preglede, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja, pri čemer po potrebi sodeluje z zadevnim subjektom;
5. zahteva informacije, ki jih potrebujejo za oceno ukrepov za obvladovanje tveganj za kibernetsko varnost, ki jih je sprejel zadevni subjekt, vključno z dokumentiranimi politikami na področju kibernetske varnosti, in izpolnjevanje obveznosti predložitve informacij pristojnim organom v skladu z 28. členom tega zakona;
6. zahteva dostop do prostorov, podatkov, dokumentov in informacij, potrebnih za opravljanje njegovih nadzornih nalog;
7. zahteva dokaze o izvajanju politik na področju kibernetske varnosti, kot so rezultati revizij varnosti, ki jih izvede preizkušeni revizor, in ustrezni dokazi v zvezi z njimi.

(3) Ciljno usmerjene revizije varnosti iz 2. točke prejšnjega odstavka temeljijo na ocenah tveganja, ki jih izvedejo pristojni nacionalni organi ali bistveni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Rezultati ciljno usmerjene revizije varnosti se dajo na voljo inšpektorju.

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

(5) Inšpektor pri izvajanju svojih pooblastil iz 5., 6. ali 7. točke drugega odstavka tega člena navede namen zahteve in opredeli zahtevane informacije.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

42. člen
(ukrepi nadzora bistvenih subjektov)

(1) Inšpektorji so pri izvajanju nadzora v zvezi z bistvenimi subjekti pooblaščeni, da:

1. izdajo opozorila o kršitvah tega zakona;
2. izdajo zavezujoča navodila, tudi v zvezi z ukrepi za preprečitev ali odpravo incidenta, roki za njihovo izvedbo in poročanjem o tem, ali odredbo, s katero od bistvenih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve tega zakona;
3. bistvenim subjektom odredijo, naj prenehajo z ravnanjem, ki krši ta zakon, in naj tega ravnanja ne ponovijo več;
4. bistvenim subjektom odredijo, naj na določen način in v določenem roku poskrbijo, da bodo njihovi ukrepi za obvladovanje tveganj za kibernetsko varnost v skladu s 20. členom tega zakona, oziroma naj izpolnijo obveznosti poročanja iz 25. in 26. člena tega zakona;
5. bistvenim subjektom odredijo, naj obvestijo fizične ali pravne osebe, v zvezi s katerimi opravljajo storitve ali izvajajo dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;
6. bistvenim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi revizije varnosti;
7. imenujejo pooblaščeno osebo z natančno opredeljenimi nalogami v določenem obdobju, ki spremlja izpolnjevanje 20., 25. in 26. člena tega zakona s strani bistvenih subjektov;
8. bistvenim subjektom odredijo, naj na določen način objavijo kršitve tega zakona;
9. naložijo globo na podlagi 53. člena tega zakona poleg katerega koli od ukrepov iz točk 1. do 8. tega odstavka.

(2) Če inšpektor ugotovi, da ukrepi iz točk 1 do 4 ali iz točke 6 prejšnjega odstavka niso bili učinkoviti, bistvenemu subjektu, ki ga takšni ukrepi zadevajo, določi rok, v katerem mora sprejeti potrebne ukrepe za odpravo 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) 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.

(6) 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 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., 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.

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 je pri izvajanju svojih nadzornih nalog pri pomembnih subjektih pooblaščen vsaj za to, da:

1. opravi inšpekcijske preglede na kraju samem in nadzor na daljavo, ki jih lahko izvede skupaj z usposobljenimi strokovnjaki;
2. zahteva izvedbo ciljno usmerjene revizije varnosti, ki jo izvede preizkušeni revizor informacijskih sistemov;
3. opravi varnostne preglede, ki temeljijo na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganja, pri čemer po potrebi sodelujejo z zadevnim subjektom;
4. zahteva informacije, ki jih potrebujejo za oceno ukrepov za obvladovanje tveganj za kibernetsko varnost, ki jih je sprejel zadevni subjekt, vključno z dokumentiranimi politikami na področju kibernetske varnosti, in izpolnjevanje obveznosti predložitve informacij pristojnim organom v skladu z 28. členom tega zakona;
5. zahteva dostop do prostorov, podatkov, dokumentov in informacij, potrebnih za opravljanje njihovih nadzornih nalog;
6. zahteva dokaze o izvajanju politik na področju kibernetske varnosti, kot so rezultati revizij varnosti, ki jih izvede preizkušeni revizor, in ustrezni dokazi v zvezi z njimi.

(3) Ciljno usmerjene revizije varnosti iz 2. točke prejšnjega odstavka temeljijo na ocenah tveganja, ki jih izvedejo pristojni nacionalni organi ali pomembni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Rezultati ciljno usmerjene revizije varnosti se dajo na voljo inšpektorju.

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

(5) Inšpektor pri izvajanju svojih pooblastil iz 4., 6. ali 7. točke drugega odstavka tega člena navede namen zahteve in opredeli zahtevane informacije.

(6) Inšpektor sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554. Pri tem inšpektor zagotovi, da o nadzoru pomembnega subjekta, ki je imenovan za ključnega tretjega ponudnika storitev IKT na podlagi člena 31 Uredbe (EU) 2022/2554, o tem obvesti nadzorniški forum, ustanovljen na podlagi člena 32(1) Uredbe (EU) 2022/2554.

(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.

44. člen
(ukrepi nadzora pomembnih subjektov)

(1) Inšpektorji so pri izvajanju nadzora v zvezi s pomembnimi subjekti pooblaščeni, da:

1. izdajo opozorila o kršitvah tega zakona;
2. izdajo zavezujoča navodila ali odredbo, s katero od pomembnih subjektov zahtevajo, da odpravijo ugotovljene pomanjkljivosti ali kršitve njihovih obveznosti določenih s tem zakona;
3. pomembnim subjektom odredijo, naj prenehajo z ravnanjem, ki ni v skladu z njihovimi obveznostmi določenimi s tem zakonom in naj tega ravnanja ne ponovijo več;
4. pomembnim subjektom odredijo, naj na določen način in v določenem roku poskrbijo, da bodo njihovi ukrepi za obvladovanje tveganj za kibernetsko varnost v skladu z 20. členom tega zakona, oziroma naj izpolnijo obveznosti poročanja iz 25. in 26. člena tega zakona;
5. pomembnim subjektom odredijo, naj obvestijo fizične ali pravne osebe, za katere opravljajo storitve ali izvajajo dejavnosti, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o vseh mogočih zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;
6. pomembnim subjektom odredijo, naj v razumnem roku izvedejo priporočila, dana na podlagi revizije varnosti;
7. pomembnim subjektom odredijo, naj na določen način objavijo kršitve tega zakona;
8. naložijo ali zahtevajo, naj ustrezni organi ali sodišča v skladu z nacionalnim pravom naložijo globo na podlagi 54. člena tega zakona, poleg katerega koli od ukrepov iz točk 1. do 7. tega odstavka.

(2) Inšpektor pri sprejemanju ukrepov iz prejšnjega odstavka tega člena spoštuje postopkovne pravice pomembnega 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 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., 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.

(3) 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.

45. člen
(ocena skladnosti)

(1) Odgovorne osebe zagotovijo, da bistveni subjekti izvajajo oceno skladnosti sprejetih ukrepov za obvladovanje tveganj kibernetske varnosti iz tega zakona in da pomembni subjekti izvajajo oceno skladnosti takšnih ukrepov.

(2) Izvajanje ocene skladnosti morajo bistveni subjekti opraviti najmanj enkrat na dve leti, pred potekom roka pa, če to zahteva inšpektor ali v primeru pojava pomembnega incidenta. Ocena skladnosti se izvaja kot revizija informacijske varnosti ali v okviru revizije poslovanja, ki se izvaja na podlagi drugih predpisov in vključuje tudi področje informacijske varnosti iz tega zakona in na podlagi tega zakona izdanih podzakonskih predpisov ali izvedbenih aktov Evropske komisije.

(3) Pomembni subjekti morajo izvesti oceno skladnosti na zahtevo inšpektorja ali v primeru pojava pomembnega incidenta.

(4) Preizkušeni revizor za bistvenega ali pomembnega subjekta pripravi poročilo o izvedeni oceni skladnosti.

(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 varnosti, ki jo zahteva inšpektor po tem zakonu, izbere preizkušenega revizorja. O svoji izbiri in o začetku postopka revizije varnosti informacijskih sistemov 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 tretjega odstavka 23. člen tega zakona;
- ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega šestega ali sedmega 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 tretjega odstavka 23. člena tega zakona,
- ne izpolni obveznosti iz prvega odstavka 24. člena tega zakona,
- ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 28. člena tega zakona
- ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 29. člena tega zakona,
- ne izpolni obveznosti iz prvega, drugega, tretjega, petega ali šestega odstavka 45. člena tega zakona,
- ne izpolni obveznosti iz tretjega odstavka 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 tretjega odstavka 23. člen tega zakona;
- ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega, šestega ali sedmega odstavka 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 tretjega odstavka 23. člena tega zakona,
- ne izpolni obveznosti iz prvega odstavka 24. člena tega zakona,
- ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 28. člena tega zakona
- ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 29. člena tega zakona,
- ne izpolni obveznosti iz prvega, drugega, tretjega, petega ali šestega odstavka 45. člena tega zakona,
- ne izpolni obveznosti iz tretjega odstavka 47. člena tega zakona.

(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).

XI. Prehodne določbe

56. člen
(vzpostavitev samoregistracije, seznamov in obveščanje)

(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz 6. člena tega zakona po prvem odstavku 7. člena tega zakona v roku dveh mesecev od uveljavitve tega zakona.
(2) Zavezanci iz 6. člena tega zakona opravijo prvo registracijo po mehanizmu za samoregistracijo v roku dveh mesecev od njegove vzpostavitve v skladu s prejšnjim odstavkom.
(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, 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, 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.

57. člen
(sprejem ukrepov za obvladovanje tveganj)

Bistveni in pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost iz 20. člena tega zakona v roku šestih mesecev od uveljavitve tega zakona.

58. 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.

59. 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.

60. 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.

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

(1) Z dnem uveljavitve tega zakona prenehajo veljati določbe 115., 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):

- v prvem odstavku 116. člena se za besedama »ta omrežja« dodata besedi »in storitve«;
- v prvem stavku drugega odstavka 116. člena se besedi »prejšnjega člena« nadomestita z besedilom: »zakona, ki ureja informacijsko varnost«;
- v prvem stavku četrtega odstavka 116. člena se besedilo »tretjega odstavka prejšnjega člena" nadomesti z besedilom »vseh varnostnih tveganj v skladu z zakonom, ki ureja informacijsko varnost« v petem odstavku 116. člena se za besedama »predmetnih omrežij« dodata besedi »in storitev«;
- v četrtem odstavku 124. člena se besedilo za vejico, ki se glasi: »se uporablja določba petega odstavka 115. člena tega zakona« nadomesti z besedilom »mora biti ta vsaj enkrat letno pregledan. Za njegovo sprejetje in morebitne spremembe ali posodobitve je potrebna predhodna odobritev pristojnih organov, odgovornih za delovanje centrov za sprejem komunikacije v sili.«;
- v 128. členu se prva vejica nadomesti s piko in briše besedilo »razen določb 120. in 121. člena tega zakona, kjer nadzor izvaja organ, pristojen za informacijsko varnost.«;
- v prvem odstavku 287. člena se brišeta besedilo »ali organa, pristojnega za informacijsko varnost na podlagi 128. člena tega zakona« prvega stavka in tretji stavek;
- v 288. členu se za besedo »Agencija« vejica nadomesti z veznikom »in«, besedilo »ter organ, pristojen za informacijsko varnost, se morajo« pa se nadomesti z besedama »se morata«;
- v 289. členu se črta tretji odstavek;
- v 299. členu se črtajo 22., 23., 24., 26., 27., 28., 29. in 30. točka.

(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 izdaje podzakonskih predpisov sprejetih na podlagi tega zakona.

62. 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«.

63. 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«.

64. 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

65. 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 (med podjetji)		— 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 motornih vozil, prikolic in polprikolic	podjetja, ki opravljajo katero koli gospodarsko 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).