Z A K O N

O INFORMACIJSKI VARNOSTI (ZINFV-1)

I. SPLOŠNE DOLOČBE

1. člen

(vsebina zakona)

(1) Ta zakon ureja področje informacijske in kibernetske varnosti ter določa 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) in skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT), ureja sprejetje Strategije kibernetske varnosti Republike Slovenije, kibernetsko obrambo ter sodelovanje pristojnih državnih organov in skupin CSIRT.

(2) Za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji ta zakon določa tudi ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost ter obveznost poročanja zavezancev po tem zakonu in prostovoljno priglasitev incidentov. Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor, vključno za certificiranje za kibernetsko varnost.

2. člen

(namen zakona)

(1) Namena zakona sta sistemska ureditev področja informacijske in kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti, vključno s krepitvijo zaupanja v proizvode informacijsko-komunikacijske tehnologije (v nadaljnjem besedilu: IKT), storitve IKT in postopke IKT ter krepitvijo njihove varnosti v Republiki Sloveniji na področjih, ki so poglavitna za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti.

(2) S tem zakonom se v pravni red Republike Slovenije prenaša Direktiva 2022/2555/EU 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 z dne 27. 12. 2022, str. 80), zadnjič popravljeno s Popravkom (UL L št. 90348 z dne 12. 6. 2024, str. 139), (v nadaljnjem besedilu: Direktiva 2022/2555/EU).

(3) S tem zakonom se ureja izvajanje Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L št. 151 z dne 7. 6. 2019, str. 15), zadnjič spremenjeno z Uredbo (EU) 2025/37 Evropskega parlamenta

in Sveta z dne 19. decembra 2024 o spremembi Uredbe (EU) 2019/881 glede upravljanih varnostnih storitev (UL L št. 2025/37 z dne 15. 1. 2025), (v nadaljnjem besedilu: Uredba 2019/881/EU).

(4) S tem zakonom se ureja izvajanje Uredbe (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov (UL L št. 202 z dne 8. 6. 2021, str. 1), (v nadaljnjem besedilu: Uredba 2021/887/EU).

(5) S tem zakonom se ureja izvajanje Uredbe (EU) 2025/38 Evropskega parlamenta in Sveta z dne 19. decembra 2024 o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskih groženj in incidentov ter pripravo in odzivanje nanje ter spremembi Uredbe (EU) 2021/694 (Akt o kibernetski solidarnosti) (UL L št. 2025/38 z dne 15. 1. 2025), (v nadaljnjem besedilu: Uredba 2025/38/EU).

3. člen

(izključitev uporabe zakona)

(1) Za bistvene in pomembne subjekte v sektorjih bančništva in infrastrukture finančnega trga iz Priloge 1 tega zakona se IV. in IX. poglavje tega zakona ne uporabljata.

(2) Ta zakon se ne uporablja za subjekte, ki jih Republika Slovenija izvzame s področja uporabe Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L št. 333 z dne 27. 12. 2022, str. 1), zadnjič spremenjene z Delegirano uredbo Komisije (EU) 2024/1774 z dne 13. marca 2024 o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo orodja, metode, postopke in politike za obvladovanje tveganj na področju IKT ter poenostavljen okvir za obvladovanje tveganj na področju IKT (UL L št. 2024/1774 z dne 25. 6. 2024), (v nadaljnjem besedilu: Uredba 2022/2554/EU) v skladu s četrtim odstavkom 2. člena navedene uredbe.

(3) Ta zakon se ne uporablja za tiste informacijsko-komunikacijske sisteme, v katerih se varujejo tajni podatki, za katere je nacionalni varnostni organ iz zakona, ki ureja tajne podatke, opravil varnostno vrednotenje in izdal varnostno dovoljenje za delovanje sistema v skladu z navedenim zakonom. Za te sisteme se uporabljajo predpisi s področja varovanja tajnih podatkov in pravila varovanja tajnih podatkov mednarodnih zvez ali organizacij, katerih članica je Republika Slovenije, ali mednarodni sporazumi s področja tajnih podatkov, ki jih je sklenila Republika Slovenija.

(4) Ne glede na prejšnji odstavek nacionalni varnostni organ iz zakona, ki ureja tajne podatke, priglaša incidente v informacijsko-komunikacijskih sistemih iz prejšnjega odstavka pristojnemu nacionalnemu organu po tem zakonu.

(5) Za avtonomni informacijski in telekomunikacijski sistem iz zakona, ki ureja obrambo, ki ni zajet v tretjem odstavku tega člena, se smiselno uporabljajo ukrepi za obvladovanje tveganj in priglasitve incidentov iz IV. poglavja tega zakona.

4. člen

(obdelava podatkov in informacij)

(1) Obdelava osebnih podatkov na podlagi tega zakona se izvaja v skladu s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev pa obdelavo osebnih podatkov izvajajo tudi v skladu s predpisom, ki ureja zasebnost na področju elektronskih komunikacij.

(2) Podatki in informacije, ki se obdelujejo na podlagi tega zakona in so opredeljeni kot tajni, poslovna skrivnost ali varovani podatki, se obravnavajo v skladu s področnimi predpisi, ki urejajo njihovo obravnavo in varovanje.

(3) Izmenjava varovanih podatkov 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 in podatkov ter se zaščitita varnost in poslovni interes zadevnih subjektov. Podrobnejše organizacijske in logično-tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenje zbirk podatkov, katerih upravljavec je pristojni nacionalni organ in vsebujejo varovane podatke pristojnega nacionalnega organa, določi vlada.

(4) Pri pošiljanju ali izmenjavi podatkov in informacij na podlagi tega zakona se upoštevajo tudi (neformalni) sporazumi o nerazkritju informacij, kot je semaforski protokol.

(5) Obveznost izmenjave podatkov in informacij zunaj Republike Slovenije na podlagi tega zakona ne velja za subjekte javne uprave, ki izvajajo dejavnosti s področja nacionalne varnosti, pri čemer bi razkritje teh podatkov in informacij ogrozilo vitalne interese Republike Slovenije.

5. člen

(pomen izrazov)

Izrazi, uporabljeni v tem zakonu, pomenijo:

1. centralni državni informacijsko-komunikacijski sistem je osrednje državno informacijsko-komunikacijsko omrežje ali sistem v upravljanju ministrstva, pristojnega za upravljanje informacijsko-komunikacijskih sistemov, in je 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 na podlagi centraliziranega upravljanja in nadzora;

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

3. digitalna storitev je katera koli storitev informacijske družbe ali katera koli storitev, ki se običajno opravi odplačno, na daljavo, elektronsko in na posamezno zahtevo prejemnika storitev;

4. dnevniški zapisi so strukturirani ali nestrukturirani zapisi dogodkov v omrežnih in informacijskih sistemih, ki omogočajo analizo in rekonstrukcijo incidentov ali skorajšnjih incidentov;

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

– storitev dostopa do interneta: ki je javno dostopna elektronska komunikacijska 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, ki so v celoti ali pretežno sestavljene iz prenosa signalov, kot so storitve prenosa, ki se uporabljajo za opravljanje storitev stroj–stroj in za radiodifuzijo;

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 in v nekaterih primerih tudi predstavnikov Evropske komisije, ki sodeluje kot opazovalka;

7. evropski certifikat kibernetske varnosti je dokument, ki potrjuje, da je bil zadevni proizvod IKT, storitev IKT ali postopek IKT ocenjen glede skladnosti s specifičnimi varnostnimi zahtevami, določenimi v evropski certifikacijski shemi za kibernetsko varnost;

8. finančna spodbuda je izvajanje financiranja v obliki nepovratnih sredstev, kritje stroškov za dobavo blaga ali storitev oziroma sofinanciranje stroškov za dobavo blaga ali storitev za zvišanje ravni kibernetske varnosti;

9. incident je dogodek, ki je 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;

10. informacijska varnost pomeni zaščito in varovanje omrežnih in informacijskih sistemov ter pripadajočih podatkov pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, in sicer za zagotavljanje zaupnosti, avtentičnosti, celovitosti in razpoložljivosti navedenih sistemov in podatkov;

11. inšpekcijski varnostni pregled je postopek, v katerem inšpektor oziroma inšpektorica (v nadaljnjem besedilu: inšpektor) pri zavezancu v postopku inšpekcijskega nadzora izvede identifikacijo in oceno morebitnih ranljivosti v omrežnih in informacijskih sistemih ter preizkus učinkovitosti varnostnih ukrepov oziroma mehanizmov in izpostavljenosti kibernetskim grožnjam, poleg tega preveri ustreznost učinkovitega zaznavanja in obravnavanja kibernetskih incidentov;

12. javno elektronsko komunikacijsko omrežje je 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;

13. kibernetska grožnja je vsaka potencialna okoliščina, dogodek ali dejanje, ki bi lahko poškodovalo, prekinilo ali drugače škodljivo vplivalo na omrežja in informacijske sisteme, uporabnike takih sistemov in druge osebe;

14. kibernetska higiena je dobra praksa ohranjanja varnosti in zaščite informacij v digitalnem okolju. To vključuje ukrepe in postopke, namenjene zaščiti računalniških sistemov, omrežij in podatkov pred varnostnimi grožnjami;

15. kibernetski incident velikih razsežnosti je incident, ki povzroči motnjo, ki presega zmožnost Republike Slovenije za odziv nanj, ali incident, ki pomembno vpliva na vsaj dve državi članici Evropske unije;

16. 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 potrebni za zaščito in varovanje kibernetskega prostora pred kibernetskimi grožnjami in incidenti;

17. kibernetski prostor je globalno informacijsko okolje, ki ga tvorijo informacijski sistemi in omrežja, podatki, digitalne naprave in njihovi uporabniki;

18. kibernetska varnost so dejavnosti, ki so potrebne za zaščito omrežnih in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje;

19. ključni deli nacionalnega varnostnega sistema so sistemi obrambe, notranje varnosti, varstva pred naravnimi in drugimi nesrečami in podsistemi sistema nacionalne varnosti, ki vključuje tudi zunanjepolitične, gospodarske, informacijske in druge dejavnosti, ki neposredno vplivajo na nacionalno varnost;

20. ključni informacijski sistemi so vsi omrežni in informacijski sistemi s pripadajočimi podatki zavezanca, brez katerih ta ne more neprekinjeno izvajati storitev iz Priloge 1 ali 2 tega zakona, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti;

21. kriza je resna grožnja 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 je storitev zaupanja, ki izpolnjuje zadevne zahteve iz zakona, ki ureja elektronsko identifikacijo in storitve zaupanja;

24. medsektorske skupnosti zavezancev so skupnosti zavezancev, ki presegajo delovanje sektorskih skupnosti zavezancev in vključujejo sodelovanje med njimi z namenom združevanja znanja in izkušenj, da bi rešili izzive, ki presegajo okvire posameznih sektorjev;

25. mreža skupin CSIRT je skupnost, ki prispeva h krepitvi zaupanja ter spodbuja hitro in učinkovito operativno sodelovanje med državami članicami Evropske unije, v kateri sodelujejo skupine CSIRT iz držav članic Evropske unije, skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije Unije (CERT-EU) in Evropska komisija kot opazovalka;

26. nadzorni informacijski sistemi so informacijski sistemi, v katerih se izvajata upravljanje in nadzor delovanja omrežij in informacijskih sistemov subjekta, vključno z zaznavanjem varnostnih dogodkov, anomalij in groženj ter odzivanjem nanje;

27. notranji revizor oziroma notranja revizorka (v nadaljnjem besedilu: notranji revizor) je preizkušeni notranji revizor oziroma preizkušena notranja revizorka (v nadaljnjem besedilu: preizkušeni notranji revizor), ki je pridobil strokovni naziv pri Slovenskem inštitutu za revizijo in je vpisan v njegov register aktivnih preizkušenih notranjih revizorjev ali oseba, ki je pridobila naziv državni notranji revizor ali preizkušeni državni notranji revizor;

28. obvladovanje incidentov so vsa dejanja in postopki, namenjeni preprečevanju, odkrivanju, analizi in zajezitvi incidentov ali odzivanju nanje ter okrevanju po njih;

29. ogrožanje vitalnih interesov Republike Slovenije je ogrožanje njene ustavne ureditve, neodvisnosti, ozemeljske celovitosti, obrambne sposobnosti in javne varnosti;

30. omrežje za dostavo vsebin je mreža geografsko porazdeljenih strežnikov za zagotavljanje visoke razpoložljivosti, dostopnosti ali hitre dostave digitalnih vsebin in storitev uporabnikom interneta v imenu ponudnikov vsebin in storitev;

31. omrežni in informacijski sistem:

– je elektronsko komunikacijsko omrežje, kot je opredeljeno v zakonu, ki ureja elektronske komunikacije,

– je vsaka naprava ali skupina med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali

– zajema digitalne podatke, ki jih elementi iz prve in druge alineje te točke shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

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

33. platforma za storitve družbenega mreženja je platforma, ki končnim uporabnikom omogoča, da se povezujejo, si izmenjujejo vsebine, se spoznavajo in komunicirajo med seboj prek več naprav ter zlasti s klepeti, objavami videoposnetki in sporočili;

34. pomembna kibernetska grožnja je kibernetska grožnja, za katero se glede na njene tehnične značilnosti lahko domneva, da bi lahko resno negativno vplivala na omrežne in informacijske sisteme subjekta ali na uporabnike njegovih storitev, tako da bi povzročila znatno premoženjsko ali nepremoženjsko škodo;

35. ponudnik kvalificiranih storitev zaupanja je ponudnik storitev zaupanja, ki zagotavlja eno ali več storitev zaupanja in mu nadzorni organ dodeli kvalificirani status;

36. ponudnik storitev sistema domenskih imen (v nadaljnjem besedilu: ponudnik storitev DNS) je 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.

37. ponudnik storitev zaupanja je fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja, kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja;

38. ponudnik upravljanih storitev je subjekt, ki opravlja storitve v zvezi z namestitvijo, upravljanjem, delovanjem ali vzdrževanjem proizvodov IKT, 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;

39. ponudnik upravljanih varnostnih storitev je ponudnik upravljanih storitev, ki izvaja ali opravlja pomoč za dejavnosti, povezane z obvladovanjem tveganj za kibernetsko varnost;

40. postopek IKT je sklop dejavnosti, ki se izvaja za zasnovo, razvoj, dobavo ali vzdrževanje proizvoda ali storitve IKT;

41. povezani subjekt je subjekt, ki se povezuje s centralnim državnim informacijsko-komunikacijskim sistemom;

42. proizvod IKT je element ali skupina elementov omrežja ali informacijskega sistema;

43. predstavnik iz V. poglavja tega zakona je fizična ali pravna oseba s sedežem v državi članici Evropske unije, pri čemer je ta oseba izrecno imenovana, da deluje v imenu ponudnika storitev DNS, registra vrhnjih domenskih (v nadaljnjem besedilu: 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 državi članici Evropske unije, s katerim lahko pristojni organ ali skupina CSIRT vzpostavi stik namesto z zadevnim subjektom v zvezi z obveznostmi zadevnega subjekta na podlagi tega zakona;

44. ranljivost je pomanjkljivost, dovzetnost ali napaka proizvoda ali storitve IKT, ki jo kibernetska grožnja lahko izkoristi;

45. raziskovalna organizacija je, ne glede na zakon, ki ureja znanstvenoraziskovalno dejavnost, subjekt, ki poglavitni del svojih dejavnosti namenja izvajanju uporabnih raziskav ali eksperimentalnemu razvoju z namenom uporabe rezultatov teh raziskav v komercialne namene, vendar ne vključuje akademskih in drugih izobraževalnih ustanov;

46. register vrhnjih domenskih imen (v nadaljnjem besedilu: register TLD imen) je 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;

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

48. revizor informacijskih sistemov je preizkušeni revizor informacijskih sistemov z ustreznim revizijskim znanjem, ki je strokovni naziv pridobil pri Slovenskem inštitutu za revizijo in je vpisan v njegov register aktivnih preizkušenih revizorjev informacijskih sistemov;

49. sektorske skupnosti zavezancev so skupine zavezancev, ki delujejo v istem sektorju in se osredotočajo na posamični sektor z namenom izmenjave informacij, sodelovanja in reševanja skupnih izzivov;

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

51. sistem domenskih imen (v nadaljnjem besedilu: DNS) je 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;

52. skorajšnji incident je 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;

53. skrbnik informacijsko-komunikacijskega sistema je oseba, odgovorna za upravljanje, vzdrževanje in zaščito informacijskega sistema v organizaciji;

54. 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 Agencije Evropske unije za kibernetsko varnost (v nadaljnjem besedilu: agencija ENISA) ter Evropske službe za zunanje delovanje kot opazovalke;

55. spletni iskalnik je digitalna 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;

56. spletna tržnica je storitev, ki uporablja programsko opremo, vključno s spletno stranjo, delom spletne strani ali aplikacije, ki jo upravlja trgovec ali nekdo v njegovem imenu, in ki potrošnikom omogoča, da sklepajo pogodbe na daljavo z drugimi trgovci ali potrošniki;

57. standard je tehnična specifikacija, ki jo je sprejel priznani organ za standardizacijo za večkratno ali stalno uporabo, s katero ni obvezna skladnost in spada v eno izmed 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;

58. stičišče omrežij je omrežna zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih omrežij (avtonomnih sistemov), predvsem zaradi izmenjave internetnega prometa, ter ki zagotavlja medsebojno povezavo zgolj avtonomnim sistemom, 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;

59. storitev IKT je storitev, ki v celoti ali pretežno zajema prenos, shranjevanje, priklic ali obdelavo informacij prek omrežij in informacijskih sistemov;

60. storitev podatkovnega centra je 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 zagotavljanje nemotene dobave električne energije in zagotavljanje zahtevanih okoljskih razmer v podatkovnem centru;

61. storitev v oblaku je digitalna 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;

62. storitev zaupanja je elektronska 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;

63. subjekt, ki opravlja storitve registracije domenskih imen, je registrar ali zastopnik, ki deluje v imenu registrarja, kot je ponudnik storitev registracije za zasebnost ali pooblaščenec ali preprodajalec;

64. subjekt je oseba javnega ali zasebnega prava;

65. subjekti javne uprave so subjekti javne uprave na državni in lokalni ravni, ki so ustanovljeni z javnopravnim aktom, razen pravosodnih organov, državnega tožilstva, Ustavnega sodišča Republike Slovenije, Državnega zbora Republike Slovenije, Državnega sveta Republike Slovenije in Banke Slovenije;

66. subjekti javne uprave na državni ravni so ministrstva, organi v njihovi sestavi, vladne službe in upravne enote ter tisti javni infrastrukturni zavodi, ki so ustanovljeni v skladu z zakonom, ki ureja znanstvenoraziskovalno in inovacijsko dejavnost. Mednje spadajo tudi drugi subjekti javne uprave iz Priloge 3, ki je kot Priloga sestavni del tega zakona;

67. subjekti javne uprave na lokalni ravni so občine;

68. tehnična specifikacija je tehnična specifikacija za informacijsko-komunikacijsko tehnologijo;

69. tretja država je država, ki ni članica Evropske unije, ali država, ki ni podpisnica Sporazuma o ustanovitvi Evropskega gospodarskega prostora (UL L št. 1 z dne 3. 1. 1994, str. 3);

70. tveganje je možnost izgube ali motnje zaradi incidenta ter je izraženo kot kombinacija razsežnosti izgube ali motnje in verjetnosti, da bi se incident zgodil;

71. varni kraj je lokacija, odporna proti okoljskim vplivom, podnebnim spremembam in drugim tveganjem, ki bi lahko ogrozili varno obravnavo incidentov ter zaščito informacij in sistemskih virov;

72. varnost omrežnih in informacijskih sistemov je 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;

73. varnostno-operativni center organa državne uprave je notranja organizacijska enota posameznega organa državne uprave, ki se odziva na incidente na področju informacijske varnosti in izpolnjuje pogoje iz tega zakona;

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

II. ZAVEZANCI

6. člen

(zavezanci)

(1) Zavezanci po tem zakonu so subjekti, ki spadajo med vrste subjektov iz Prilog 1 ali Priloge 2, ki sta kot Prilogi sestavni del tega zakona (v nadaljnjem besedilu: Priloga 1 ali 2 tega zakona), če imajo:

– vsaj 50 zaposlenih in

– letni promet ali letno bilančno vsoto vsaj 10 milijonov eurov.

(2) Subjekti iz prejšnjega odstavka so zavezanci po tem zakonu ne glede na število zaposlenih ali letni promet ali letno bilančno vsoto, če:

1. storitev opravljajo kot:

   – ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev,

   – ponudniki storitev zaupanja,

   – registri TLD imen in ponudniki storitev DNS;

2. je subjekt edini ponudnik storitve ali dejavnosti v Republiki Sloveniji, katere izvajanje ga uvršča med vrste subjektov iz Priloge 1 ali 2;

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 sistemsko tveganje, zlasti za sektorje iz Priloge 1 ali 2, v katerih bi lahko taka motnja imela čezmejni vpliv;

5. ima subjekt poseben pomen na državni ali lokalni ravni za posamezni sektor iz Priloge 1 ali 2 ali za izvajanje posamezne storitve, ki ga uvršča med vrste subjektov iz Priloge 1 ali 2 ali zaradi medsebojne odvisnosti z drugimi sektorji iz Prilog 1 ali 2 v Republiki Sloveniji;

6. gre za subjekt javne uprave na državni ravni.

(3) Ne glede na prvi in drugi odstavek tega člena so zavezanci po tem zakonu tudi:

1. subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo;

2. subjekti, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost;

3. subjekti, ki so v državnih načrtih zaščite in reševanja opredeljeni kot službe državnega pomena, če bi nedelovanje njihovih omrežnih in informacijskih sistemov ogrozilo izvajanje nalog zaščite in reševanja iz prej navedenih načrtov, in

4. mestne občine kot subjekti javne uprave na lokalni ravni.

(4) Ne glede na prejšnje odstavke so za izvajanje 27. člena tega zakona, ki se nanaša na certificiranje za kibernetsko varnost, zavezane tudi druge fizične in pravne osebe, ki spadajo na področje uporabe Uredbe 2019/881/EU, in sicer v delu navedene uredbe, ki ureja certifikacijski okvir za kibernetsko varnost.

(5) Ne glede na prejšnje odstavke Banka Slovenije ni zavezanec po tem zakonu.

7. člen

(bistveni in pomembni subjekti)

(1) Zavezanci iz prejšnjega člena, razen subjektov iz 2. točke tretjega odstavka in četrtega odstavka, se delijo na bistvene in pomembne subjekte.

(2) Bistveni subjekti so:

1. vrste subjektov iz Priloge 1, ki imajo vsaj 250 zaposlenih ali letni promet vsaj 50 milijonov eurov ali letno bilančno vsoto vsaj 43 milijonov eurov,

2. ponudniki kvalificiranih storitev zaupanja in registri TLD 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 ali letno bilančno vsoto vsaj 10 milijonov eurov,

4. subjekti javne uprave na državni ravni,

5. vse druge vrste subjektov iz Priloge 1 tega zakona, ki jih na podlagi 2. do 5. točke drugega odstavka prejšnjega člena 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 iz sektorja 9. Upravljanje storitev IKT iz Priloge 1 in niso subjekti iz 1. do 6. točke tega odstavka, ki jih na predlog pristojnega nacionalnega organa določi vlada.

(3) Pomembni subjekti so:

– vrste subjektov iz Priloge 2 tega zakona, vključno s tistimi, ki jih na podlagi 2. do 5. točke drugega odstavka prejšnjega člena in na predlog pristojnega nacionalnega organa določi vlada z odločbo,

– subjekti iz 3. točke tretjega odstavka prejšnjega člena, ki jih na predlog pristojnega nacionalnega organa določi vlada z odločbo. Pristojni nacionalni organ pripravi predlog na podlagi pobude Uprave Republike Slovenije za zaščito in reševanje, ki vsebuje poimenski seznam zadevnih subjektov, in

– drugi subjekti ali organi iz prejšnjega člena, ki niso bistveni subjekti na podlagi prejšnjega odstavka.

(4) Za izvajanje 7. točke drugega odstavka tega člena Banka Slovenije, Agencija za trg vrednostnih papirjev in Agencija za zavarovalni nadzor pošljejo pristojnemu nacionalnemu organu poimenski seznam subjektov, ki izvajajo storitve upravljanja storitev IKT iz Priloge 1 tega zakona na področju sektorja 3. Bančništvo ali 4. Infrastrukture finančnega trga iz Priloge 1.

(5) Zoper odločbe iz 5. točke drugega odstavka in iz prve ter druge alineje tretjega odstavka tega člena ni dovoljena pritožba, dovoljen pa je upravni spor.

8. člen

(samoregistracija in seznam zavezancev)

(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz 6. člena tega zakona, razen za zavezance iz četrtega odstavka 6. člena tega zakona in za subjekte iz prvega odstavka 3. člena tega zakona.

(2) Zavezanci, za katere je vzpostavljen mehanizem za samoregistracijo iz prejšnjega odstavka, se morajo prek tega mehanizma registrirati v tridesetih dneh od dneva, ko so nastopile okoliščine, na podlagi katerih izpolnjujejo merila iz 6. in 7. člena tega zakona. Ne glede na to tridesetdnevni rok za samoregistracijo za tiste zavezance, ki jim je bila vročena odločba iz 5. točke drugega odstavka ali iz prve ali druge alineje tretjega odstavka prejšnjega člena, teče od dneva vročitve odločbe. Zavezanci ob samoregistraciji podajo vsaj naslednje informacije:

1. o imenu in naslovu, kontaktnih podatkih, matični številki in elektronskem naslovu zavezanca za vročanje,

2. o ustreznem sektorju in podsektorju iz Priloge 1 ali 2 tega zakona, v katerem zavezanec izvaja vrste storitev iz teh prilog, ali kategorijo zavezancev, ki niso vključeni v navedenih prilogah, so pa zavezanci na podlagi tretjega odstavka 6. člena tega zakona,

3. navedbo, ali ima subjekt vsaj 50 zaposlenih in letni promet ali bilančno vsoto vsaj 10.000.000,00 eura,

4. navedbo, ali ima subjekt vsaj 250 zaposlenih ali letni promet vsaj 50.000.000,00 eura ali letno bilančno vsoto vsaj 43.000.000,00 eura,

5. o kontaktni osebi za informacijsko varnost in njenem namestniku ter njune kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami,

6. o dodeljenih blokih javnih naslovov IP,

7. o seznamu držav članic Evropske unije, kjer opravljajo storitve, ki spadajo na področje uporabe tega zakona, ter

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

(3) Ne glede na nabor informacij iz prejšnjega odstavka subjekti iz prvega odstavka 32. člena tega zakona ob samoregistraciji iz prejšnjega odstavka podajo v njem navedeni nabor informacij.

(4) Na podlagi informacij zavezancev iz drugega ali tretjega odstavka tega člena in ob upoštevanju drugega in tretjega odstavka prejšnjega člena pristojni nacionalni organ vzpostavi seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Ta seznam, ki vsebuje informacije zavezancev iz drugega ali tretjega odstavka tega člena, je varovani podatek pristojnega nacionalnega organa in ga pristojni nacionalni organ redno ali vsaj vsaki dve leti pregleda in po potrebi posodobi. Pristojni nacionalni organ omogoči dostop do seznama v delu, ki se nanaša na zavezance iz njihove pristojnosti, tudi pristojnim skupinam CSIRT.

(5) Zavezanci iz drugega odstavka tega člena z uporabo mehanizma za samoregistracijo sporočijo morebitne spremembe podatkov, ki so jih predložili na podlagi drugega ali tretjega odstavka tega člena, najpozneje v desetih delovnih dneh od datuma spremembe. Na seznam iz prejšnjega odstavka se zadevne spremembe prenesejo nemudoma.

(6) Ne glede na prejšnji odstavek subjekt iz drugega odstavka tega člena, ki presodi, da ne spada več med zavezance, o tem in razlogih za takšno presojo obvesti pristojni nacionalni organ, ki preveri njegove navedbe in ob potrditvi razlogov v mehanizmu za samoregistracijo in na seznamu iz četrtega odstavka tega člena pri zadevnem subjektu zaznamuje, da ta subjekt ni več zavezanec, in o tem obvesti zadevni subjekt. V primeru, da zavezanec, ki mu je bila izdana odločba iz 5. točke drugega odstavka ali iz prve ali druge alineje tretjega odstavka prejšnjega člena, meni, da ne izpolnjuje več pogojev za njeno izdajo, o tem obvesti pristojni nacionalni organ, ki ob potrditvi prenehanja teh pogojev predlaga vladi razveljavitev njene zadevne odločbe. Če vlada zadevno odločbo razveljavi, pristojni nacionalni organ po tem, ko mu je razveljavitvena odločba vročena, pri zadevnem subjektu zaznamuje, da ta subjekt ni več zavezanec, in o tem obvesti zadevni subjekt.

(7) Ne glede na drugi odstavek tega člena Banka Slovenije, Agencija za trg vrednostnih papirjev in Agencija za zavarovalni nadzor pošljejo pristojnemu nacionalnemu organu poimenski seznam finančnih subjektov iz Uredbe 2022/2554/EU, ki so subjekti iz prvega odstavka 3. člena tega zakona, v tridesetih dneh od njihove prepoznave. V enakem roku obvestijo pristojni nacionalni organ o spremembi seznama.

(8) Pristojni nacionalni organ informacije iz prejšnjega odstavka nemudoma vključi na seznam iz četrtega odstavka tega člena.

(9) Za potrebe izvajanja tega člena pristojni nacionalni organ brezplačno pridobiva podatke zavezancev iz drugega odstavka tega člena iz zbirke podatkov Poslovni register Slovenije upravljavca Agencije Republike Slovenije za javnopravne evidence in storitve.

III. ORGANIZACIJA NACIONALNEGA SISTEMA INFORMACIJSKE VARNOSTI

9. člen

(strategija kibernetske varnosti)

(1) Vlada sprejme strategijo kibernetske varnosti (v nadaljnjem besedilu: strategija), ki je okvir za izvedbo ukrepov za vzpostavitev učinkovitega nacionalnega sistema zagotavljanja informacijske oziroma kibernetske varnosti. V strategijo se vključijo:

1. cilji in prednostne naloge strategije;

2. okvir upravljanja za dosego ciljev in izvedbo prednostnih nalog iz prejšnje točke, vključno s politikami iz drugega odstavka tega člena;

3. okvir upravljanja, ki opredeljuje vloge in odgovornosti ustreznih zainteresiranih deležnikov kibernetske varnosti na državni ravni, podpira sodelovanje in usklajevanje na državni ravni med pristojnim nacionalnim organom, enotno kontaktno točko in skupinami CSIRT iz tega zakona ter podpira 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 odzivanje na incidente in okrevanje 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 pristojnim nacionalnim organom 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;

8. okvir politike za okrepljeno usklajevanje med pristojnim nacionalnim organom iz tega zakona in organom, ki je po odločitvi vlade osrednji organ za spremljanje in koordinacijo odzivanja na hibridne grožnje v Republiki Sloveniji (v nadaljnjem besedilu: osrednji organ za odzivanje na hibridne grožnje), za namene izmenjave informacij o tveganjih, kibernetskih grožnjah in incidentih ter o nekibernetskih tveganjih, grožnjah in incidentih, ki bi nakazovali hibridno delovanje;

9. načrt, vključno s potrebnimi ukrepi, za povečanje splošne ozaveščenosti državljanov o kibernetski varnosti.

(2) Strategija vključuje naslednje politike:

1. o obravnavanju kibernetske varnosti v dobavni verigi proizvodov in storitev IKT, ki jih subjekti uporabljajo za opravljanje svojih storitev;

2. o vključitvi in specifikaciji zahtev za proizvode in storitve IKT pri javnem naročanju, povezanih s kibernetsko varnostjo, vključno v zvezi s certificiranjem za kibernetsko varnost, šifriranjem in uporabo odprtokodnih proizvodov za kibernetsko varnost;

3. o obvladovanju ranljivosti, vključno s spodbujanjem in omogočanjem usklajenega razkrivanja ranljivosti na podlagi prvega odstavka 17. člena tega zakona;

4. povezane z ohranjanjem splošne razpoložljivosti, celovitosti in zaupnosti javnega jedra odprtega interneta, vključno s kibernetsko varnostjo podmorskih komunikacijskih kablov;

5. o spodbujanju razvoja in vključevanja ustreznih naprednih tehnologij za izvajanje najsodobnejših ukrepov za obvladovanje tveganj na področju kibernetske varnosti;

6. o spodbujanju in razvoju izobraževanja in usposabljanja na področju kibernetske varnosti, spretnosti na področju kibernetske varnosti, okrepitve ozaveščanja, raziskovalnih in razvojnih pobud na področju kibernetske varnosti ter smernic o dobrih praksah in nadzoru kibernetske higiene, namenjenih državljanom, deležnikom in subjektom;

7. o podpiranju akademskih in raziskovalnih institucij pri razvoju in izboljševanju orodij kibernetske varnosti in varne omrežne infrastrukture ter spodbujanju njihovega uvajanja;

8. o vključevanju ustreznih postopkov in primernih orodij za podpiranje prostovoljne izmenjave informacij o kibernetski varnosti med subjekti v skladu s pravom Evropske unije;

9. o krepitvi 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. o spodbujanju aktivne kibernetske zaščite.

(3) Pristojni nacionalni organ v treh mesecih od sprejetja strategije iz tega člena o tem obvesti Evropsko komisijo. Pri tem lahko izključi informacije iz 5., 7. in 8. točke prvega odstavka, ki so pomembne za nacionalno varnost.

(4) Pristojni nacionalni organ sprotno in redno vsaj vsakih pet let oceni strategijo na podlagi ključnih kazalnikov uspešnosti, ki izhajajo iz doseganja ciljev in prednostnih nalog strategije.

10. člen

(pristojni nacionalni organ)

(1) Pristojni nacionalni organ je Urad Vlade Republike Slovenije za informacijsko varnost.

(2) Pristojni nacionalni organ izvaja 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 ali nadzorniki sektorjev iz Prilog 1 in 2 tega zakona, z Informacijskim pooblaščencem, z organi kazenskega pregona in 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, v skladu s Kazenskim zakonikom;

7. koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za okrepitev 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 in varnostne dokumentacije zavezancev;

11. pregleduje ustreznost določitve zavezancev iz 5. točke drugega odstavka in prve ter druge alineje tretjega odstavka 7. člena tega zakona vsaj vsaki dve leti in lahko vladi predlaga posodobitev seznama zavezancev;

12. za statistične namene in namene seznanjanja javnosti dvakrat letno pripravi anonimizirane informacije o priglašenih incidentih, te nato javno objavi na osrednjem spletnem mestu državne uprave;

13. strokovne in svetovalne naloge in naloge koordinatorja na področju odnosov z javnostmi, ki zajemajo komunikacijo z zunanjimi in notranjimi javnostmi ter krizno komuniciranje v primeru incidenta;

14. v sodelovanju s službo vlade, pristojno za komuniciranje z javnostmi, izdela in vzdržuje nacionalni načrt komuniciranja v primeru incidentov;

15. je enotna kontaktna točka, ki ima na področju kibernetske varnosti in obrambe povezovalno vlogo za zagotavljanje čezmejnega sodelovanja z drugimi državami in mednarodnimi organizacijami;

16. predstavlja in zastopa interese Republike Slovenije v delovnih skupinah na področju kibernetske varnosti in obrambe v okviru Sveta Evropske unije, Evropske komisije, agencije ENISA, zveze NATO in drugih mednarodnih organizacij;

17. imenuje in napotuje svoje predstavnike v delovne skupine, odbore in mreže na področju kibernetske varnosti in obrambe v okviru Sveta Evropske unije, Evropske komisije, agencije ENISA, zveze NATO in drugih mednarodnih organizacij;

18. je član Skupine za sodelovanje, v katero imenuje svoje predstavnike, in zagotovi razmere za njihovo učinkovito in uspešno delovanje;

19. imenuje predstavnike v mrežo EU-CyCLONe;

20. sodeluje pri aktivaciji nudenja in sprejemanja pomoči za obvladovanje kriz v skladu z mednarodnimi pogodbami in dogovori;

21. imenuje predstavnika v upravni odbor agencije ENISA in sodeluje pri njenem delu;

22. izpolnjuje druge obveznosti iz neposredno uporabljivih aktov Evropske unije s področja kibernetske varnosti;

23. izpolnjuje obveznosti obveščanja Evropske komisije, agencije ENISA, zveze NATO in Skupine za sodelovanje ter obveznosti obveščanja preostalih mednarodnih organizacij;

24. vodi medresorsko koordinacijsko delovno skupino za mednarodno sodelovanje na področju kibernetske varnosti in obrambe;

25. opravlja druge naloge mednarodnega sodelovanja;

26. opravlja naloge inšpekcijskega nadzora po tem zakonu prek Inšpekcije za informacijsko varnost, ki je njegova notranja organizacijska enota;

27. pripravlja predloge predpisov s področja informacijske in kibernetske varnosti;

28. opravlja naloge nacionalnega certifikacijskega organa za kibernetsko varnost;

29. je Nacionalni koordinacijski center za kibernetsko varnost;

30. kot prejemnik ali dodeljevalec sredstev se vključuje v programe financiranja na nacionalni ravni in na ravni Evropske unije ter drugih mednarodnih povezav za področje informacijske in kibernetske varnosti;

31. dodeljuje finančne spodbude za izvedbo izbranih projektov za področje informacijske in kibernetske varnosti;

32. financira kadrovske štipendije za delo v pristojnem nacionalnem organu, v skladu z zakonom, ki ureja štipendiranje;

33. odloča o sodelovanju pri medsebojnih strokovnih pregledih;

34. določi enotno informacijsko varnostno politiko, razen za informacijsko-komunikacijske sisteme, namenjene področjem obrambe, varstva pred naravnimi in drugimi nesrečami, policije, internega informacijskega sistema notranjih zadev, obveščevalno-varnostne dejavnosti, zunanjih zadev, preprečevanja in odkrivanja pranja denarja in financiranja terorizma ter opravljanja plačilnega prometa za proračunske uporabnike, in

35. je Nacionalno kibernetsko vozlišče v skladu s prvim, drugim in tretjim odstavkom 4. člena Uredbe 2025/38/EU, ki sodeluje v čezmejnem kibernetskem vozlišču na podlagi četrtega odstavka navedenega člena te uredbe in v evropskem sistemu za opozarjanje na področju kibernetske varnosti iz 3. člena navedene uredbe, in

36. opravlja druge naloge, določene s tem zakonom ali z drugimi predpisi.

11. člen

(nacionalni koordinacijski center za kibernetsko varnost)

(1) Pristojni nacionalni organ je Nacionalni koordinacijski center za kibernetsko varnost (v nadaljnjem besedilu: NCC-SI) in je v tej vlogi pristojen za izvajanje nalog iz Uredbe (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov (UL L št. 202 z dne 8. 6. 2021, str. 1).

(2) NCC-SI v skladu z uredbo EU iz prejšnjega odstavka izvaja naloge za krepitev kibernetske varnosti, vključno s spodbujanjem raziskav, tehnološkega razvoja in industrijske zmogljivosti na tem področju, ter sodeluje z Evropskim centrom za kibernetsko varnost in drugimi nacionalnimi koordinacijskimi centri za kibernetsko varnost držav članic Evropske unije.

12. člen

(organ za obvladovanje kibernetskih kriz)

(1) Pristojni organ za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz (v nadaljnjem besedilu: organ za obvladovanje kibernetskih kriz) v Republiki Sloveniji je pristojni nacionalni organ, ki je v tej vlogi pristojen za sodelovanje v mreži 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).

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

1. cilji nacionalnih ukrepov in dejavnosti za pripravljenost,

2. naloge in odgovornosti organov za obvladovanje kibernetskih incidentov, kibernetskih incidentov velikih razsežnosti in 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 usposabljanjem,

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 in

8. postopki sodelovanja med organom za obvladovanje kibernetskih kriz in osrednjim organom za odzivanje na hibridne grožnje z namenom učinkovitega usklajevanja pri odzivanju na hibridne grožnje.

(4) Organ za obvladovanje kibernetskih kriz ob zaznavi kibernetskih incidentov, za katere presodi, da lahko povzročijo krizo, nemudoma obvesti Svet za nacionalno varnost (v nadaljnjem besedilu: SNAV) in osrednji organ za odzivanje na hibridne grožnje. V sodelovanju s prizadetimi zavezanci po tem zakonu, pristojnimi področnimi regulatorji in zadevnimi nosilci sektorjev kritične infrastrukture iz zakona, ki ureja kritično infrastrukturo, in osrednjim organom za odzivanje na hibridne grožnje analizira stanje ter z ugotovitvami seznanja SNAV in mu po potrebi predlaga ukrepe. SNAV na podlagi predpisa, ki ureja področje kriznega upravljanja in vodenja kriz, izdela oceno situacije. Na podlagi ocene svetuje vladi o nadaljnjih ukrepih.

(5) Vlada lahko na predlog SNAV 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 v skladu z zakonom, ki ureja Vlado Republike Slovenije.

(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 podatki in informacije iz petega odstavka 4. člena tega zakona.

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

13. člen

(skupine za odzivanje na incidente na področju računalniške varnosti)

(1) Skupine CSIRT in njihove pristojnosti za obravnavo incidentov posameznih skupin zavezanih subjektov določi vlada. Med tako določenimi skupinami CSIRT vlada določi tudi skupino CSIRT, ki je koordinator za usklajeno razkrivanje ranljivosti v Republiki Sloveniji po 17. členu tega zakona.

(2) Skupine CSIRT morajo izpolnjevati zahteve iz 14. člena tega zakona in so pristojne za obravnavo incidentov v skladu s postopkom, določenim s tem zakonom.

(3) Skupine CSIRT izmenjujejo informacije z bistvenimi in pomembnimi subjekti ter drugimi ustreznimi deležniki z uporabo ustrezne, varne in odporne komunikacijske in informacijske infrastrukture, ki jo vzpostavi pristojni nacionalni organ, poleg tega sodelujejo s pristojnim nacionalnim organom pri uvajanju in uporabi orodij za varno izmenjavo informacij.

(4) Skupine CSIRT medsebojno sodelujejo in si v skladu s 34. členom tega zakona izmenjujejo ustrezne informacije s sektorskimi ali medsektorskimi skupnostmi zavezancev.

(5) Skupine CSIRT sodelujejo pri medsebojnih strokovnih pregledih v skladu z 19. členom tega zakona.

(6) Skupine CSIRT sodelujejo v mreži skupin CSIRT, lahko pa tudi v drugih mrežah za mednarodno sodelovanje.

(7) Skupine CSIRT lahko sodelujejo s skupinami CSIRT iz tretjih držav. Pri tem s temi skupinami iz tretjih držav lahko izmenjujejo informacije z uporabo ustreznih protokolov, vključno s semaforskim protokolom, da se zagotovi uspešen, učinkovit in varen način izmenjave informacij. Skupine CSIRT si lahko izmenjujejo ustrezne informacije s skupinami CSIRT iz tretjih držav, vključno z osebnimi podatki, v skladu z določbami 10. poglavja Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22).

(8) Skupine CSIRT lahko sodelujejo s skupinami CSIRT iz tretjih držav ali enakovrednimi organi tretjih držav, zlasti za zagotavljanje pomoči na področju kibernetske varnosti.

(9) 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 nemudoma obvesti Evropsko komisijo. Evropsko komisijo obvesti tudi o identiteti skupine CSIRT, ki je imenovana za koordinatorja iz prvega odstavka 17. člena tega zakona.

14. člen

(zahteve in tehnične zmogljivosti skupin CSIRT)

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

1. zagotavljajo visoko stopnjo razpoložljivosti lastnih 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. Pri tem jasno opredelijo komunikacijske kanale ter o njih obvestijo uporabnike in partnerje;

2. prostori in podporni informacijski sistemi so 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, in

6. imajo nadomestne sisteme in nadomestni delovni prostor, da se zagotovi neprekinjeno izvajanje njihovih storitev.

15. člen

(naloge skupin CSIRT)

(1) Skupine CSIRT iz prvega odstavka 13. člena tega zakona na področjih, za katera so pristojne, izvajajo naslednje naloge:

1. spremljanje in analiziranje kibernetskih groženj, ranljivosti in incidentov na državni ravni, na zahtevo bistvenih in pomembnih subjektov pa jim nudijo pomoč v zvezi s sprotnim spremljanjem njihovih omrežnih in informacijskih sistemov;

2. zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o kibernetskih grožnjah, ranljivostih in incidentih zadevnim bistvenim in pomembnim subjektom, pristojnemu nacionalnemu organu in drugim pristojnim organom, osrednjim organom za odzivanje na hibridne grožnje in drugim ustreznim deležnikom, če je mogoče, takoj;

3. odzivanje na incidente in zagotavljanje pomoči zadevnim bistvenim in pomembnim subjektom;

4. zbiranje in analiziranje forenzičnih podatkov in opravljanje dinamičnih analiz tveganja in incidentov ter situacijsko zavedanje na področju kibernetske varnosti;

5. na zahtevo bistvenega ali pomembnega subjekta opravljanje proaktivnega pregleda omrežnih in informacijskih sistemov zadevnega subjekta, da se odkrijejo ranljivosti, ki bi lahko imele pomemben negativen 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 tretjega odstavka 13. člena tega zakona in

8. zagotavljanje medsebojne pomoči in sodelovanje z drugimi organi, ki so na podlagi predpisov pristojni za obravnavanje incidentov.

(2) Skupine CSIRT lahko z namenom odkrivanja ranljivosti omrežnih in informacijskih sistemov, ki niso konfigurirani na varen način, ter za obveščanje zadevnih subjektov s ciljem odpravljanja varnostnih groženj izvajajo proaktivno in nevsiljivo pregledovanje javno dostopnih omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov, za katere so pristojne. Takšno pregledovanje ne sme negativno vplivati na delovanje storitev teh subjektov.

(3) Pri izvajanju nalog iz prvega odstavka tega člena lahko skupine CSIRT na podlagi pristopa, ki temelji na tveganjih, prednostno razvrščajo naloge.

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

(5) Skupine CSIRT nemudoma obvestijo pristojni nacionalni organ o lastnem incidentu, ki bi lahko vplival ali vpliva na delovanje in razpoložljivost njihovih storitev, ki jih zagotavljajo 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 37. člena tega zakona.

(7) Skupina CSIRT iz prvega odstavka 13. člena, ki je pristojna za obravnavo incidentov subjektov javne uprave na državni in lokalni ravni, je za namen učinkovitega izvajanja nalog informacijske in kibernetske varnosti ter kibernetske obrambe pooblaščena za neposredni, nujni in sorazmerni vpogled v delovanje informacijske infrastrukture centralnega državnega informacijsko-komunikacijskega sistema. Upravljavec centralnega državnega informacijsko-komunikacijskega sistema mu mora to omogočiti.

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

(9) Skupine CSIRT iz prvega odstavka 13. člena tega zakona izvajajo tudi programe ozaveščanja v skladu s strategijo kibernetske varnosti.

16. člen

(sodelovanje skupin CSIRT z deležniki iz zasebnega sektorja)

(1) Skupine CSIRT iz prvega odstavka 13. člena tega zakona za dosego ciljev tega zakona sodelujejo s subjekti iz zasebnega sektorja. V ta namen lahko sklepajo tudi dogovore o sodelovanju.

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

– postopki obvladovanja incidentov,

– obvladovanjem kriz in

– usklajenim razkrivanjem ranljivosti na podlagi prvega odstavka 17. člena tega zakona.

(3) Skupina CSIRT, ki zazna ranljivost informacijsko-komunikacijskega sistema subjekta iz prvega odstavka tega člena, tega o tem nemudoma obvesti.

17. člen

(usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti)

(1) Skupina CSIRT iz prvega odstavka 13. člena tega zakona, ki je določena za koordinatorja za usklajeno razkrivanje ranljivosti v Republiki Sloveniji (v nadaljnjem besedilu: koordinator), deluje kot zaupanja vreden posrednik in po potrebi olajšuje sodelovanje med fizično ali pravno osebo, ki poroča o ranljivostih, in proizvajalcem ali ponudnikom proizvodov 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 kot koordinatorke imenovane v okviru mreže skupin CSIRT.

(4) Koordinator v zvezi s sporočenimi ranljivostmi sodeluje tudi z agencijo ENISA.

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

18. člen

(sodelovanje na nacionalni ravni)

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

1. med seboj sodelujejo pri izpolnjevanju obveznosti;

2. sodelujejo z Javno agencijo za civilno letalstvo Republike Slovenije, Upravo Republike Slovenije za jedrsko varnost, 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 s področij, ki jim pripadajo zavezanci iz 6. člena tega zakona;

3. sodelujejo z organi kazenskega pregona in Informacijskim pooblaščencem, če to ne škoduje izvajanju pristojnosti nadzora ali odločanja teh organov;

4. 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 ter o nekibernetskih tveganjih, grožnjah in izrednih dogodkih na področju kritične infrastrukture, ki vplivajo na bistvene subjekte, opredeljene kot kritični subjekti na podlagi zakona, ki ureja kritično infrastrukturo, ter o ukrepih, sprejetih v odziv na takšna tveganja, grožnje, incidente in izredne dogodke;

5. redno sodelujejo z osrednjim organom za odzivanje na hibridne grožnje in si izmenjujejo informacije o tveganjih, kibernetskih grožnjah in incidentih ter o nekibernetskih tveganjih, grožnjah in incidentih, ki bi nakazovali hibridno delovanje, ter o ukrepih, sprejetih v odziv na takšna tveganja, grožnje in incidente, in

6. redno izmenjujejo informacije, tudi o relevantnih incidentih in kibernetskih grožnjah z Inšpekcijo za informacijsko družbo, Informacijskim pooblaščencem, Banko Slovenije, Javno agencijo za civilno letalstvo Republike Slovenije, Agencijo za komunikacijska omrežja in storitve Republike Slovenije, nacionalnim varnostnim organom za varovanje tajnih podatkov na podlagi zakona, ki ureja tajne podatke, in drugimi področnimi regulatorji.

(2) Medsebojna izmenjava informacij o incidentih, kibernetskih grožnjah in skorajšnjih incidentih iz 29. in 35. člena tega zakona med pristojnim nacionalnim organom, enotno kontaktno točko, skupinami CSIRT iz tega zakona in pristojnimi organi iz 4., 5. in 6. točke prejšnjega odstavka se izvaja z uporabo digitalne platforme pristojnega nacionalnega organa iz desetega odstavka 30. člena tega zakona.

19. člen

(medsebojni strokovni pregled)

(1) Pristojni nacionalni organ lahko 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 iz drugih držav članic Evropske unije.

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

1. raven izvajanja zahtev glede obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja iz 21., 22., 29. in 30. člena tega zakona,

2. raven zmogljivosti, vključno z razpoložljivimi finančnimi, tehničnimi in človeškimi viri, in učinkovitost opravljanja nalog pristojnega nacionalnega organa,

3. operativne zmogljivosti skupin CSIRT,

4. raven izvajanja medsebojne pomoči iz 51. člena tega zakona,

5. raven izvajanja dogovorov o izmenjavi informacij o kibernetski varnosti iz 34. člena tega zakona in

6. posebni čezmejni ali medsektorski vidiki, ki jih opredeli pristojni nacionalni organ.

(3) Za izvajanje medsebojnih strokovnih pregledov iz prvega odstavka tega člena se uporablja metodologija Skupine za sodelovanje, pri čemer pristojni nacionalni organ to metodologijo objavi na osrednjem spletnem mestu državne uprave.

(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 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 Skupina za sodelovanje določi ob pomoči Evropske komisije in agencije ENISA. Rezultate samoocene nato pošlje 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 ne glede na 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 osebam. Kot podlago za delovne metode strokovnjakov za kibernetsko varnost upoštevajo tudi kodekse ravnanja, ki jih je pripravila Skupina za sodelovanje in jih je pristojni nacionalni organ objavil na osrednjem spletnem mestu državne uprave.

(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 agenciji 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 iz druge države članice Evropske unije in jo o tem obvesti na način iz prejšnjega odstavka. Pri tem pristojni nacionalni organ sporoči razloge za nasprotovanje imenovanju posameznih strokovnjakov, razen če so razlogi povezani z nacionalno varnostjo.

(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. Pristojni nacionalni organ se v primerih iz prvega odstavka tega člena lahko odloči, da poročilo na osrednjem spletnem mestu državne uprave objavi v celoti ali njegovo redigirano različico.

IV. UKREPI ZA OBVLADOVANJE TVEGANJ IN PRIGLASITVE INCIDENTOV

20. člen

(upravljanje)

(1) Za izvajanje ukrepov iz 21. in 22. člena tega zakona so odgovorni predstojniki subjektov javne uprave, in odgovorne osebe pravnih oseb, to so fizične osebe, ki vodijo,

nadzorujejo ali upravljajo poslovanje pravne osebe oziroma so po zakonu, aktu o ustanovitvi ali pooblastilu pristojne in dolžne zagotoviti zakonito delovanje (v nadaljnjem besedilu: odgovorne osebe) bistvenih ali pomembnih subjektov.

(2) Odgovorne osebe iz prejšnjega odstavka odobrijo ukrepe za obvladovanje tveganj iz 22. člena tega zakona, ki jih subjekt izvaja zaradi izpolnjevanja obveznosti, določenih s tem zakonom, in nadzirajo njihovo izvajanje.

(3) Odgovorne osebe iz prvega odstavka tega člena se najmanj vsaka štiri leta izobražujejo oziroma usposabljajo na področju obvladovanja tveganj informacijske in kibernetske varnosti ter njihovega vpliva na dejavnosti ali storitve, ki jih izvaja subjekt.

(4) Odgovorne osebe zagotavljajo redno usposabljanje zaposlenih, da pridobijo dovolj znanj in spretnosti, s katerimi se usposobijo za prepoznavanje tveganj za informacijsko in kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja subjekt. Pristojni nacionalni organ objavi na osrednjem spletnem mestu državne uprave priporočene vsebine rednega usposabljanja zaposlenih.

(5) Odgovorne osebe zagotavljajo, da vsi skrbniki informacijsko-komunikacijskih sistemov zavezanca opravijo redno letno usposabljanje, da pridobijo in ohranijo raven znanj in spretnosti ter so usposobljeni za prepoznavanje in ocenjevanje tveganj ter za oceno praks obvladovanja tveganj za informacijsko in kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja subjekt.

(6) Pristojni nacionalni organ je pristojen za organiziranje usposabljanja odgovornih oseb iz prvega odstavka tega člena. Program in način izvajanja usposabljanja odgovornih oseb na področju informacijske in kibernetske varnosti določi vlada na predlog pristojnega nacionalnega organa.

(7) Pristojni nacionalni organ vodi seznam odgovornih oseb iz prvega odstavka tega člena, ki so opravile usposabljanje iz prejšnjega odstavka. Seznam obsega ime in priimek osebe, enotno matično številko občana in datum opravljenega usposabljanja.

21. člen

(varnostna dokumentacija)

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

1. politiko ali področne politike o varnosti omrežnih in informacijskih sistemov,

2. natančen in posodobljen popis informacijskih in drugih sredstev in podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, ter njihove upravljavce;

3. analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije;

4. politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij ter določitvijo vlog in odgovornosti;

5. načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;

6. načrt odzivanja na incidente s protokolom obveščanja pristojne skupine CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente ter opisom vlog in odgovornosti za odzivanje na incidente;

7. načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za informacijsko in kibernetsko varnost, pri čemer ta načrt upošteva tveganja in področne posebnosti bistvenega ali pomembnega subjekta in

8. politiko s postopki za presojo učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

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

(3) Če ima bistveni ali pomembni subjekt za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo za potrebe izvajanja tega zakona dopolni, kot je to potrebno.

(4) Bistveni subjekt, ki je povezani subjekt po tem zakonu, in zanj ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, na podlagi prvega odstavka v povezavi z drugim odstavkom 74.a člena Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23; v nadaljnjem besedilu: ZDU-1) izvaja naloge iz prvega odstavka 74.a člena ZDU-1, izvede popis informacijskih sredstev iz 1. točke prvega odstavka tega člena in vanj vključi najmanj tista informacijska sredstva, ki podpirajo njegove glavne ali pomembne storitve in procese za zagotovitev povezave s centralnim državnim informacijsko-komunikacijskim omrežjem ali sistemom. Bistveni subjekt izvede popis v sodelovanju z ministrstvom, pristojnim za upravljanje informacijsko-komunikacijskih sistemov, ki mu mora na zahtevo poslati ustrezne podatke, s katerimi razpolaga, in sicer v tridesetih dneh od prejema posamičnega zahtevka.

(5) Ne glede na določbe tega člena bistveni in pomembni subjekti, na katere se nanašajo izvedbeni akti Evropske komisije iz prvega pododstavka petega odstavka 21. člena Direktive 2022/2555/EU ali iz drugega pododstavka petega odstavka 21. člena Direktive 2022/2555/EU, uporabljajo določbe izvedbenega akta glede varnostne dokumentacije zadevnih subjektov.

22. člen

(ukrepi za obvladovanje tveganj)

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

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

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

1. podporo vodstva subjekta pri zagotavljanju informacijske in kibernetske varnosti ter vključitev področja informacijske in kibernetske varnosti v letni načrt poslovanja ali letni program dela,

2. zagotavljanje integritete kadrov v povezavi z informacijsko in kibernetsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve v skladu s 23. členom tega zakona,

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

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

5. izvajanje in upravljanje varnostnih kopij podatkov,

6. zagotavljanje in ohranjanje dnevniških zapisov o delovanju omrežnih in informacijskih sistemov v skladu s 24. členom tega zakona,

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

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

9. upravljanje prometa in komunikacij,

10. varnost dobavne verige z določitvijo ustreznih minimalnih zahtev, povezanih z informacijsko in kibernetsko varnostjo, za ključne dobavitelje ali ponudnike storitev, pri čemer se zahteve nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev, in to v skladu s četrtim odstavkom tega člena,

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

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

13. upravljanje in preprečevanje izrab tehničnih ranljivosti,

14. zaščito pred zlonamerno programsko kodo ter način zaznavanja poskusov vdorov in preprečevanja incidentov,

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

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

17. politike in postopke v zvezi z uporabo oblačnih storitev, ki jih uporabljajo za svoje delovanje ali opravljanje storitev.

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

– stopnjo izpostavljenosti tveganjem,

– velikost subjekta,

– verjetnost pojava incidentov in

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

(4) Bistveni in pomembni subjekti morajo pri presoji in izvedbi ustreznih varnostnih ukrepov za varnost dobavne verige upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev, ter splošno kakovost proizvodov in praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Ugotavljati morajo, kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige, poleg tega lahko preverjajo njihovo izvajanje pri dobaviteljih in ponudnikih storitev. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih Skupina za sodelovanje pripravi v sodelovanju z Evropsko komisijo in agencijo ENISA v skladu s prvim odstavkom 22. člena Direktive 2022/2555/EU.

(5) Bistveni ali pomembni subjekti morajo najmanj enkrat letno ali v rednih obdobjih, ki jih opredelijo v politiki in postopkih za presojo učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost, in ob zaznanih ranljivostih preverjati izpolnjevanje varnostnih ukrepov iz drugega odstavka tega člena. V primeru ugotovljenega pomanjkljivega ali neustreznega izvajanja varnostnih ukrepov morajo nemudoma 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 sprejetju varnostnih ukrepov iz drugega odstavka tega člena upoštevajo izvedbene akte Evropske komisije iz prvega pododstavka petega odstavka 21. člena Direktive 2022/2555/EU.

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

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

(9) 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, pristojne za posamezni ključni del nacionalnovarnostnega sistema.

(10) Upravljavec centralnega državnega informacijsko-komunikacijskega sistema mora povezanim subjektom določiti minimalne varnostne zahteve informacijske in kibernetske varnosti. Za pravočasno odzivanje na kibernetske grožnje in preprečevanje škodljivih posledic morebitnega težjega ali kritičnega incidenta ter za izvajanje kibernetske obrambe je upravljavec centralnega državnega informacijsko-komunikacijskega sistema pooblaščen, da izvede ustrezne, nujne in sorazmerne ukrepe za zaščito centralnega državnega informacijsko-komunikacijskega sistema. Ukrepi vključujejo tudi začasni odklop posameznega povezanega subjekta iz centralnega državnega informacijsko-komunikacijskega sistema, dokler ugotovljena tveganja niso odpravljena.

(11) Bistveni subjekt iz četrtega odstavka prejšnjega člena sprejme ukrepe iz 1. do 4. točke drugega odstavka tega člena. Preostale ukrepe iz drugega odstavka tega člena pa sprejme le za morebitne informacijsko-komunikacijske sisteme, ki jih upravlja. Pri tem mora upoštevati tudi minimalne varnostne zahteve za povezane subjekte upravljavca centralnega državnega informacijsko-komunikacijskega sistema iz prejšnjega odstavka.

(12) Bistveni subjekti, ki so na podlagi zakona, ki ureja kritično infrastrukturo, določeni kot kritični subjekti in spadajo med vrste subjektov iz sektorja 8. Digitalna infrastruktura iz Priloge 1 tega zakona, se za zagotovitev varnostnih ukrepov varovanja iz 11. točke drugega odstavka tega člena na predlog nosilca sektorja kritične infrastrukture za digitalno infrastrukturo v skladu s predpisi, ki urejajo zasebno varovanje, določijo za zavezance obveznega organiziranja varovanja, ki morajo kritično infrastrukturo varovati v skladu z navedenimi predpisi.

(13) Varnostni ukrepi iz drugega odstavka tega člena morajo biti:

1. učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje;

2. prilagojeni tako, da se prizadevanja bistvenih in pomembnih subjektov usmerijo v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost, in se izogibajo podvajanjem;

3. skladni tako, da se prednostno obravnavajo osnovne in skupne varnostne ranljivosti bistvenih in pomembnih subjektov kljub področnim posebnostim, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna področja,

4. sorazmerni s tveganji tako, da se izogiba čezmerni obremenitvi posameznega bistvenega ali pomembnega subjekta;

5. konkretni tako, da bistveni in pomembni subjekti te varnostne ukrepe izvajajo in da ti ukrepi prispevajo h krepitvi njihove informacijske varnosti in

6. preverljivi tako, da se na zahtevo pristojnega organa lahko predložijo dokazila o njihovi izvedbi.

23. člen

(preverjanje preteklosti)

(1) Bistveni ali pomembni subjekt lahko ob upoštevanju ocene tveganja preveri preteklost zaposlenih in kandidatov za zaposlitev na delovnih mestih, pomembnih za opravljanje storitev subjekta, ki imajo ali bodo imeli pooblastilo za neposredni ali oddaljeni dostop do njegovih ključnih informacijskih sistemov. V skladu z oceno tveganja lahko preveri preteklost tudi za zaposlene pri pogodbenih izvajalcih. Preverjanje preteklosti se opravi za zadnjih pet let.

(2) Preverjanje preteklosti osebe iz prejšnjega odstavka se po njenem predhodnem soglasju opravi tako, da se:

– potrdi identiteta osebe, katere preteklost se preverja, in

– preverijo kazenske evidence Republike Slovenije, držav članic Evropske unije in tretjih držav glede zapisov pravnomočnih kazenskih obsodb za kazniva dejanja, ki se preganjajo po uradni dolžnosti in ki so po presoji bistvenega ali pomembnega subjekta sporna z vidika opravljanja nalog na zadevnem delovnem mestu ali za izvedbo pogodbenih obveznosti, in sicer s področja terorizma ter kršitev zoper življenje in telo, človekove pravice in svoboščine, človekovo zdravje, delovno razmerje in socialno varnost, premoženje, gospodarstvo, pravni promet, uradno dolžnost, javna pooblastila in javna sredstva, javni red in mir, splošno varnost ljudi in premoženja, varnost javnega prometa, okolje, prostor in naravne dobrine, suverenost Republike Slovenije, njeno obrambno moč in mednarodno pravo ter z drugih področij, razen če z zakonom, ki ureja preverjanje preteklosti za posamezni sektor iz Prilog 1 in 2 tega zakona, ni določeno drugače.

(3) Če oseba iz prejšnjega odstavka ne da soglasja za preverjanje preteklosti, se ji delo na delovnih mestih in v prostorih iz prvega odstavka tega člena ne dovoli oziroma se pogodba ne sklene.

(4) Za namen preverjanja preteklosti iz drugega odstavka tega člena smejo bistveni in pomembni subjekti zbirati naslednje podatke:

– ime in priimek osebe,

– EMŠO ali rojstni datum,

– številka uradnega identifikacijskega dokumenta, s katerim je potrjena identiteta osebe in

– podatek o nekaznovanosti ali pravnomočni obsodbi za kaznivo dejanje iz druge alineje drugega odstavka tega člena.

Osebni podatki iz tega odstavka se hranijo pet let od konca koledarskega leta, v katerem so bili zbrani, nato se nepovratno izbrišejo oziroma uničijo.

(5) Organi, organizacije in drugi subjekti, ki na podlagi zakona vodijo zbirke podatkov iz prejšnjega odstavka, morajo bistvenim in pomembnim subjektom na podlagi pisne ali s pisno obliko izenačene zahteve, v kateri je navedena ustrezna pravna podlaga za predložitev podatkov in ustrezna številka ali druga oznaka zahteve, brezplačno poslati zahtevane osebne in druge podatke.

24. člen

(dnevniški zapisi)

(1) Bistveni in pomembni subjekti določijo postopke in ustrezna orodja za spremljanje in beleženje dogodkov v svojih omrežjih in informacijskih sistemih oziroma zagotovijo zbiranje in ohranjanje dnevniških zapisov, da bi zaznali ali odkrili dogodke, ki bi se lahko šteli za incidente ali skorajšnje incidente, in se ustrezno odzvali za ublažitev njihovega negativnega učinka. Dnevniški zapisi morajo biti zbrani in ohranjeni v obsegu in na način, ki omogoča rekonstrukcijo in analizo incidentov ali skorajšnjih incidentov.

(2) Dnevniški zapisi iz prejšnjega odstavka obsegajo vsaj:

1. izhodni in vhodni omrežni promet,

2. ustvarjanje, spreminjanje ali brisanje uporabnikov omrežnih in informacijskih sistemov zadevnih subjektov ter razširitev dovoljenj,

3. dostop do sistemov, aplikacij in baz podatkov,

4. dogodke, povezane z avtentikacijo,

5. vse privilegirane dostope do sistemov in aplikacij ter dejavnosti, ki jih izvajajo upraviteljski računi,

6. dostop ali spremembe kritičnih konfiguracijskih in varnostnih datotek,

7. zapise dogodkov in zapise iz varnostnih orodij, kot so protivirusni programi, sistemi za odkrivanje vdorov ali požarni zidovi,

8. uporabo sistemskih virov in njihovo zmogljivost,

9. dostop do omrežne opreme in naprav ter njihovo uporabo in

10. aktiviranje, zaustavitev in prekinitev sistemskih storitev in beleženja zapisov.

(3) Dnevniški zapisi iz prejšnjega odstavka morajo biti hranjeni na način, ki zagotavlja njihovo avtentičnost, celovitost, razpoložljivost in zaupnost. Bistveni in pomembni subjekti zagotovijo, da imajo vsi sistemi sinhronizirane časovne vire, da se za presojo dogodkov lahko izvede korelacija dnevniških zapisov med sistemi.

(4) Bistveni in pomembni subjekti zagotavljajo ohranjanje dnevniških zapisov iz prvega odstavka tega člena za najmanj šest 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.

(5) Ohranjanje dnevniških zapisov bistvenih subjektov, ki so na podlagi zakona, ki ureja kritično infrastrukturo, določeni kot kritični subjekti, se zagotavlja na ozemlju Republike Slovenije, druga kopija pa se lahko zagotavlja na ozemlju države članice EU.

(6) Ne glede na prejšnji odstavek lahko subjekti s področja sektorjev digitalne infrastrukture, bančništva in infrastrukture finančnega trga zagotovijo ohranjanje dnevniških zapisov v celoti na ozemlju države članice EU, ob upoštevanju predpisov s področja varstva osebnih podatkov ter na podlagi ocene tveganj opredeljenih in uvedenih sorazmernih varnostnih kontrol pa tudi zunaj ozemlja držav članic EU.

(7) Ne glede na peti odstavek tega člena se dnevniški zapisi ključnih delov nacionalnega varnostnega sistema hranijo le na ozemlju Republike Slovenije.

(8) Ne glede na prejšnji odstavek lahko ministrstvo, pristojno za zunanje zadeve, hranjenje dnevniških zapisov zagotavlja tudi na diplomatskih predstavništvih in konzulatih Republike Slovenije v tujini.

(9) Ne glede na drugi odstavek tega člena bistveni in pomembni subjekti, ki so 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, glede obsega dnevniških zapisov upoštevajo določbe o spremljanju in vodenju dnevnikov iz izvedbenega akta Evropske komisije iz prvega pododstavka petega odstavka 21. člena Direktive 2022/2555 /EU.

25. člen

(ocena in samoocena skladnosti)

(1) Bistveni subjekti morajo oceno skladnosti izvajati najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta. Ocena skladnosti se izvaja kot revizija skladnosti s predpisi s področja informacijske varnosti ali v okviru notranje revizije, ki se izvaja na podlagi drugih predpisov in vključuje področje informacijske varnosti iz tega zakona in na podlagi tega zakona izdanih podzakonskih predpisov ali izvedbenih aktov Evropske komisije. Oceno skladnosti lahko v okviru notranje revizije poleg revizorjev informacijskih sistemov izvajajo tudi notranji revizorji v sodelovanju z veščakom za informacijsko tehnologijo, ki je posameznik oziroma posameznica ali organizacija, ki ima izkazano poglobljeno strokovno znanje na področju informacijsko-komunikacijskih tehnologij, katerega ali katere delo revizor uporabi kot strokovno pomoč pri pridobivanju zadostnih in ustreznih revizijskih dokazov. Revizor informacijskih sistemov ali notranji revizor pripravi poročilo o izvedeni oceni skladnosti.

(2) Če poročilo o izvedeni oceni skladnosti iz prejšnjega odstavka vsebuje ugotovitve neskladnosti in priporočila revizorja informacijskih sistemov za njihovo odpravo, bistveni subjekt pripravi načrt za odpravo ugotovljenih neskladnosti, določi način njihove odprave in roke za izvedbo.

(3) Pomembni subjekti izvedejo samooceno skladnosti najmanj enkrat na dve leti ali v primeru pojava pomembnega incidenta. Samoocena skladnosti se izvede na način, da se dokumentirano preverita skladnost pomembnega subjekta z njegovo varnostno dokumentacijo in izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost. Samoocena skladnosti se lahko izvede tudi v okviru notranje revizije.

(4) Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt izpolnjuje zahteve, predpisane s tem zakonom, ta sestavi izjavo o skladnosti, pri čemer ta vsebuje potrebne elemente samoocenjevanja skladnosti, ki omogočajo izvedbo ponovljivosti opravljene ocene.

(5) Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomembni subjekt ne izpolnjuje predpisanih zahtev, ta sestavi izjavo o ugotavljanju neskladnosti, v kateri navede ugotovljene neskladnosti in način njihove odprave z roki za izvedbo.

26. člen

(obveza predložitve podatkov in informacij)

(1) Bistveni in pomembni subjekti morajo pristojnemu nacionalnemu organu na podlagi pisne zahteve predložiti podatke in informacije, ki jih ta potrebuje za izvajanje svojih pristojnosti po tem zakonu, in sicer v roku, ki ga določi v svoji pisni zahtevi.

(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.

(3) Če pristojni nacionalni organ zahteva podatke in informacije, ki so pri subjektih iz prvega odstavka tega člena opredeljeni kot tajni ali kot poslovna skrivnost ali druga oblika varovanih podatkov, se za predložitev takšnih podatkov in informacij pristojnemu nacionalnemu organu uporabljajo izključno varne komunikacijske poti.

27. člen

(certificiranje)

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

(2) Pristojni nacionalni organ je pristojni nacionalni certifikacijski organ za kibernetsko varnost iz prvega odstavka 58. člena Uredbe 2019/881/EU.

(3) Samoocenjevanje skladnosti, za katero je v celoti odgovoren proizvajalec ali ponudnik proizvodov, storitev ali postopkov IKT, in izdaja izjave EU o skladnosti se izvajata v skladu s 53. členom Uredbe 2019/881/EU.

(4) Naloge nacionalnega akreditacijskega organa iz Uredbe 2019/881/EU v Republiki Sloveniji opravlja javni zavod Slovenska akreditacija, ta tudi akreditira organe za ugotavljanje skladnosti, ki izpolnjujejo pogoje iz navedene uredbe.

(5) Organ za ugotavljanje skladnosti v Republiki Sloveniji se določi po postopku in na način iz IV. poglavja Zakona o tehničnih zahtevah za proizvode in o ugotavljanju skladnosti (Uradni list RS, št. 17/11 in 29/23), pri čemer ta organ izpolnjuje zahteve po prej navedenem zakonu in dodatne zahteve iz priloge Uredbe 2019/881/EU.

(6) Organ za ugotavljanje skladnosti iz prejšnjega odstavka lahko na podlagi Uredbe 2019/881/EU izda evropski certifikat kibernetske varnosti, ki se nanaša na osnovno ali znatno raven zanesljivosti, in to na podlagi meril, vključenih v evropsko certifikacijsko shemo za kibernetsko varnost.

(7) Ne glede na prejšnji odstavek je v primeru, ko evropska certifikacijska shema za kibernetsko varnost določa, da lahko evropske certifikate kibernetske varnosti izdajajo izključno javni organi, za izdajo takšnih certifikatov v Republiki Sloveniji pristojen organ za ugotavljanje skladnosti iz petega odstavka tega člena, če je ta organ subjekt javnega prava. Če takšnega organa ni, je za izdajo teh certifikatov pristojen nacionalni certifikacijski organ za kibernetsko varnost.

(8) Kadar evropska certifikacijska shema za kibernetsko varnost zahteva visoko raven zanesljivosti, lahko v Republiki Sloveniji evropski certifikat kibernetske varnosti na podlagi te sheme izda nacionalni certifikacijski organ za kibernetsko varnost.

(9) Ne glede na sedmi in osmi odstavek tega člena lahko evropski certifikat kibernetske varnosti izda organ za ugotavljanje skladnosti, če nacionalni certifikacijski organ za kibernetsko varnost to predhodno odobri za vsak posamezni evropski certifikat kibernetske varnosti posebej ali na podlagi splošnega prenosa naloge izdajanja takih evropskih certifikatov kibernetske varnosti na organ za ugotavljanje skladnosti.

(10) Nacionalni certifikacijski organ za kibernetsko varnost lahko na podlagi predhodnega soglasja vlade prenese pooblastilo za izdajanje evropskih certifikatov kibernetske varnosti za visoko raven zanesljivosti iz svoje pristojnosti tudi na pristojni nacionalni certifikacijski organ za kibernetsko varnost druge države članice Evropske unije. V tem primeru nacionalni certifikacijski organ odloči o priznanju tako izdanega evropskega certifikata kibernetske varnosti za visoko raven zanesljivosti.

(11) Nacionalni certifikacijski organ za kibernetsko varnost odloča o vlogah za priznanje evropskega certifikata kibernetske varnosti, ki ga imajo fizične ali pravne osebe in so podale vlogo za takšno priznanje v Republiki Sloveniji. Poleg tega lahko z odločbo prekliče evropski certifikat kibernetske varnosti, ki ga izda pristojni organ iz šestega, sedmega ali desetega odstavka tega člena, kadar tak certifikat ni v skladu z Uredbo 2019/881/EU ali z evropskimi certifikacijskimi shemami za kibernetsko varnost, sprejetimi na podlagi 49. člena Uredbe 2019/881/EU.

(12) Fizične in pravne osebe, ki so stranke ali stranski udeleženci postopka iz šestega, sedmega ali osmega odstavka tega člena, lahko pri organu, pristojnem za izdajo evropskega certifikata kibernetske varnosti, vložijo pritožbo zoper evropski certifikat kibernetske varnosti ali zoper molk organa. Kadar se pritožba nanaša na evropski certifikat kibernetske varnosti, ki ga je izdal organ za ugotavljanje skladnosti v skladu s sedmim odstavkom tega člena, se takšna pritožba vloži pri nacionalnem certifikacijskem organu za kibernetsko varnost.

(13) Organ, pri katerem je bila vložena pritožba, preizkusi vsebino pritožbe in obvesti pritožnika o poteku postopka ali o odstopu pritožbe v reševanje nacionalnemu certifikacijskemu organu za kibernetsko varnost, ki odloči o pritožbi. Zoper odločbo pritožbenega organa je dovoljen upravni spor.

(14) Kadar na podlagi sedmega ali osmega odstavka tega člena o izdaji evropskega certifikata kibernetske varnosti odloča nacionalni certifikacijski organ za kibernetsko varnost, je zoper evropski certifikat kibernetske varnosti ali zoper molk organa dovoljen upravni spor.

(15) Sodno varstvo iz trinajstega in štirinajstega odstavka tega člena vključuje tudi nepravilno izdajo, opustitev izdaje ali priznanje evropskega certifikata kibernetske varnosti, ki ga imajo fizične ali pravne osebe, ki so stranke ali stranski udeleženci postopka, in molk organa.

(16) Za obvladovanje tveganj za varnost omrežij in informacijskih sistemov bistveni in pomembni subjekti pri izvajanju ukrepov iz 22. člena tega zakona prednostno uporabljajo kvalificirane storitve zaupanja in tiste proizvode, storitve ali postopke IKT, ki so jih razvili bistveni ali pomembni subjekti ali so bili kupljeni pri drugih subjektih in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi 49. člena Uredbe 2019/881/EU.

28. člen

(standardizacija)

(1) Bistveni in pomembni subjekti za zagotovitev skladnega izvajanja ukrepov iz 21. in 22. člena tega zakona v največji možni meri in skladno z najboljšimi razpoložljivimi praksami

ter tudi priporočili in smernicami agencije ENISA uporabljajo evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov.

(2) Pristojni nacionalni organ na osrednjem spletnem mestu državne uprave objavlja ustrezne informacije o evropskih in mednarodnih standardih in tehničnih specifikacijah, ki obravnavajo varnost omrežnih in informacijskih sistemov iz prejšnjega odstavka, ter ozavešča zavezance glede njihove uporabe.

(3) Za nadgradnjo ravni kibernetske varnosti bistvenih in pomembnih subjektov regulativni organi ali nadzorniki, ki so pristojni za sektorje iz Prilog 1 in 2 tega zakona, na osrednjem spletnem mestu državne uprave objavljajo tehnično specifične industrijske standarde in tehnične specifikacije, ki se štejejo kot priporočila.

29. člen

(obveznost priglašanja in obveščanja)

(1) Bistveni in pomembni subjekti pristojni skupini CSIRT nemudoma v skladu s prvim in drugim odstavkom 30. člena tega zakona in nacionalnim načrtom odzivanja iz drugega odstavka 12. člena tega zakona priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Pri tem se incident šteje za pomembnega (v nadaljnjem besedilu: pomemben incident), če:

– je zadevnemu subjektu povzročil ali bi mu lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube ali

– 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 vrednotenju pomembnosti incidenta upoštevajo prizadetost omrežnih in informacijskih sistemov, zlasti njihov pomen pri zagotavljanju storitev subjekta, resnost in tehnične značilnosti kibernetske grožnje in njenega vpliva na uporabnike, ranljivosti, ki se izkoriščajo, in izkušnje subjekta s podobnimi incidenti. Pri priglašanju iz prejšnjega odstavka upoštevajo izvedbene akte Evropske komisije iz prvega pododstavka enajstega odstavka 23. člena Direktive 2022/2555/EU, 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 in 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/EU, v katerih so zanje podrobneje določeni posamezni primeri, ko se incident šteje za pomembnega.

(4) Bistveni in pomembni subjekti iz prvega odstavka tega člena, ki niso subjekti iz prejšnjega odstavka, upoštevajo izvedbene akte Evropske komisije iz drugega pododstavka enajstega odstavka 23. člena Direktive 2022/2555/EU. 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 ta ugotovi čezmejni vpliv pomembnega incidenta. V primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta se ustrezna informacija pravočasno sporoči enotni kontaktni točki v skladu s 30. členom tega zakona.

(6) Bistveni in pomembni subjekti uporabnike svojih storitev nemudoma obvestijo o pomembnih incidentih iz prvega odstavka tega člena, ki bodo verjetno negativno vplivali na zagotavljanje teh storitev.

(7) Bistveni in pomembni subjekti nemudoma uporabnikom svojih storitev, ki bi jih pomembna kibernetska grožnja lahko prizadela, sporočijo vse ukrepe ali sredstva, ki jih lahko ti uporabniki sprejmejo v odziv na to grožnjo. Zadevne uporabnike obvestijo tudi o zadevni pomembni kibernetski grožnji.

(8) Ne glede na šesti in sedmi odstavek tega člena bistveni in pomembni subjekti ne obveščajo uporabnikov svojih storitev v primerih, v katerih bi bilo takšno obveščanje v nasprotju z drugim ali tretjim odstavkom 4. člena tega zakona, in v primerih, v katerih jim takšno navodilo dá pristojna skupina CSIRT ali pristojni nacionalni organ, ker bi razkritje podatkov lahko škodilo preiskavi incidenta ali nacionalni varnosti.

(9) Bistveni in pomembni subjekti, ki delujejo v sistemih, ki spadajo med ključne dele nacionalnega varnostnega sistema, izvajajo obveznosti iz tega člena ob upoštevanju obdelave informacij in podatkov, ki so predmet nacionalne varnosti v skladu s področnimi predpisi.

(10) Incidenti v informacijsko-komunikacijskih sistemih, določenih s predpisi, ki urejajo tajne podatke, se štejejo za pomembne incidente po tem zakonu in jih nacionalni varnostni organ iz zakona, ki ureja tajne podatke, na način iz prvega odstavka 30. člena tega zakona priglasi pristojnemu nacionalnemu organu.

30. člen

(postopek priglasitve pomembnih incidentov)

(1) Bistveni in pomembni subjekti za priglasitev pomembnih incidentov iz prvega odstavka prejšnjega člena pristojni skupini CSIRT predložijo:

1. nemudoma, najpozneje pa v 24 urah po zaznavi pomembnega incidenta, zgodnje sporočilo, iz katerega je po potrebi razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem in ali bi lahko imel čezmejni vpliv;

2. nemudoma, najpozneje pa v 72 urah po zaznavi pomembnega incidenta, priglasitev incidenta, s katero se po potrebi posodobijo informacije iz prejšnje točke in se 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, in to najpozneje v enem mesecu po predložitvi priglasitve incidenta iz 2. točke tega odstavka, ki vključuje:

   – podroben opis incidenta, vključno z njegovo resnostjo in vplivom,

   – vrsto grožnje ali temeljnega vzroka, ki je verjetno povzročil incident,

   – izvedene blažilne ukrepe in take ukrepe, ki se izvajajo, in

   – po potrebi čezmejni vpliv incidenta.

5. v primeru pomembnega incidenta, ki ob predložitvi končnega poročila iz prejšnje točke še vedno poteka, priglasitveni subjekt predloži poročilo o napredku, končno poročilo pa najpozneje en mesec po rešitvi incidenta.

(2) Ne glede na 2. točko prejšnjega odstavka mora ponudnik storitev zaupanja v zvezi s pomembnimi incidenti, ki vplivajo na zagotavljanje njegovih storitev, o tem nemudoma, najpozneje pa v 24 urah po zaznavi pomembnega incidenta, priglasi incident pristojni skupini CSIRT.

(3) Pristojna skupina CSIRT nemudoma in po možnosti v 24 urah po prejemu zgodnjega sporočila 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. Ob tem brez nepotrebnega odlašanja s priglasitvijo seznani pristojni nacionalni organ in ga obvešča o opravljenih aktivnostih. Na zahtevo zadevnega subjekta zagotovi dodatno tehnično podporo. Kadar obstajajo razlogi za sum, da ima incident znake kaznivega dejanja, 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 meni, da je to potrebno, zlasti kadar pomemben incident zadeva dve ali več držav članic Evropske unije, enotna kontaktna točka na zahtevo nemudoma o pomembnem incidentu obvesti enotne kontaktne točke drugih prizadetih držav članic in agencijo ENISA. To obvestilo vključuje vrsto informacij, prejetih v skladu s prvim odstavkom tega člena. Pri tem enotna kontaktna točka zaščiti varnost in poslovne interese zavezanca ter zaupnost predloženih informacij, ki jih ta zagotovi v svoji priglasitvi.

(5) Enotna kontaktna točka vsake tri mesece predloži zbirno poročilo agenciji ENISA, vključno z anonimiziranimi in zbirnimi podatki o incidentih, pomembnih kibernetskih grožnjah in skorajšnjih incidentih, priglašenih v skladu s prvim odstavkom tega člena in 35. členom tega zakona.

(6) Kadar je ozaveščenost javnosti potrebna za preprečitev pomembnega incidenta ali obravnavo pomembnega incidenta, ki še poteka, 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. Predlog za takšno obveščanje lahko pristojnemu nacionalnemu organu poda tudi pristojna skupina CSIRT.

(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, in zadevnemu nosilcu sektorja kritične infrastrukture iz navedenega zakona informacije o pomembnih incidentih, incidentih, kibernetskih grožnjah in skorajšnjih incidentih, ki so jih v skladu prvim odstavkom 29. člena tega zakona ali pri prostovoljni priglasitvi iz 35. 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. Pristojni nacionalni organ o incidentu, ki bi lahko imel večji medsektorski vpliv oziroma bi lahko ob daljšem trajanju poslabšal stabilnost nacionalne varnosti Republike Slovenije, obvesti Nacionalni center za krizno upravljanje, ustanovljen v skladu z zakonom, ki ureja Vlado Republike Slovenije, in osrednji organ za odzivanje na hibridne grožnje, ob tem lahko obvesti tudi druge pristojne organe, s katerimi sodeluje na nacionalni ravni, v skladu z 18. členom tega zakona.

(10) Priglasitve pomembnih incidentov in medsebojno sodelovanje iz tega člena se izvajajo tudi po namenski digitalni platformi, ki jo vzpostavi pristojni nacionalni organ in po kateri poteka tudi izmenjava informacij med sodelujočimi organi na podlagi drugega odstavka 18. člena tega zakona. Sodelujoči organi imajo dostop do informacij o priglasitvah subjektov, ki so povezane z njihovim področjem dela.

(11) V postopku priglašanja incidentov iz desetega odstavka prejšnjega člena se smiselno uporablja prvi odstavek tega člena.

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

– skupen seznam pomembnih incidentov, ki vsebuje podatke iz končnih poročil o incidentih iz tega člena, in

– seznam omrežnih in informacijskih sistemov, delov omrežja in digitalnih oziroma elektronskih komunikacijskih storitev zavezancev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti, ki je varovani podatek pristojnega nacionalnega organa.

(13) Za namen obravnavanja priglašenih incidentov, izvajanja blažilnih ukrepov, zagotavljanja varnosti omrežja in informacij ter preprečevanja nezakonitih ali zlonamernih dejanj, ki ogrožajo dostopnost, avtentičnost, celovitost in zaupnost informacijskih sistemov, delov omrežja ali podatkov bistvenih in pomembnih subjektov, smeta pristojna skupina CSIRT in pristojni nacionalni organ zbirati in obdelovati naslednje podatke:

– ime in priimek osebe,

– EMŠO ali rojstni datum,

– elektronski naslov osebe,

– telefonska številka osebe,

– IP naslov (statični ali dinamični),

– MAC naslov ali podoben identifikator naprave,

– uporabniško ime in geslo,

– imena aliasov, psevdonimnih identitet ali drugih vzdevkov, ki jih osebe uporabljajo v spletu

– metapodatke datotek (ki lahko vsebujejo npr. podatke o avtorju datoteke, poteh datotek, časovnih conah, jezikovnih nastavitev in drugih podatkov) in

– druge podatke, ki lahko pripomorejo k obravnavi priglašenih incidentov (npr. nize uporabniških agentov, nameščene pisave in vtičnike, identifikatorje piškotkov, naslove kripto denarnic, ipd.).

Tako pridobljeni osebni podatki se hranijo največ tri leta po preteku koledarskega leta, v katerem so bili pridobljeni, po preteku tega roka pa se izbrišejo oziroma uničijo.

(14) Za izvajanje nalog iz prejšnjega odstavka se smeta seznama iz dvanajstega odstavka tega člena povezovati s seznamom iz četrtega odstavka 8. člena tega zakona.

V. PRISTOJNOST IN REGISTRACIJA

31. člen

(pristojnost in teritorialnost)

(1) Zavezanci iz 6. člena tega zakona, ki jih je ustanovila Republika Slovenija ali imajo sedež v Republiki Sloveniji, spadajo v pristojnost pristojnega nacionalnega organa in pristojnih skupin CSIRT v skladu s tem zakonom, razen:

– ponudnikov javnih elektronskih komunikacijskih omrežij ali ponudnikov javno dostopnih elektronskih komunikacijskih storitev, ki spadajo v pristojnost pristojnih organov države članice Evropske unije, v kateri zagotavljajo svoje storitve, in

– ponudnikov storitev DNS, registrov TLD imen, subjektov, ki opravljajo storitve registracije domenskih imen, ponudnikov storitev računalništva v oblaku, ponudnikov storitev podatkovnih centrov, ponudnikov omrežij za dostavo vsebine, ponudnikov upravljanih storitev, ponudnikov upravljanih varnostnih storitev ter ponudnikov spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, ki spadajo v pristojnost pristojnih organov države članice Evropske unije, v kateri imajo glavni sedež v Evropski uniji, v skladu z drugim odstavkom tega člena.

(2) Za namene tega zakona se za subjekte iz druge alineje prejšnjega odstavka šteje, da imajo glavni sedež 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 Evropske unije, 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) To, da subjekt imenuje predstavnika iz druge alineje prvega odstavka tega člena, ne izključuje možnosti uvedbe sodnih postopkov, ki se v Republiki Sloveniji lahko uvedejo proti subjektu.

(5) Če pristojni nacionalni organ prejme zahtevek za medsebojno pomoč na podlagi 51. člena tega zakona v zvezi s subjektom iz druge alineje prvega odstavka tega člena, lahko inšpektor za informacijsko varnost v mejah zahtevka sprejme ustrezne nadzorne in izvršilne ukrepe v zvezi z zadevnim subjektom, ki opravlja storitve ali ima omrežni in informacijski sistem na ozemlju Republike Slovenije.

32. člen

(zbiranje informacij za register ponudnikov storitev pri agenciji ENISA)

(1) Subjekti, ki spadajo v pristojnost pristojnega nacionalnega organa v skladu s prvim odstavkom prejšnjega člena in so ponudniki storitev DNS, registrov TLD imen, registracije domenskih imen ali storitev računalništva v oblaku, storitev podatkovnih centrov, omrežij za dostavo vsebine, upravljanih storitev, upravljanih varnostnih storitev ter spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, pristojnemu nacionalnemu organu za olajšanje 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 1 ali 2 tega zakona,

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 prejšnjega člena,

4. posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjekta in po potrebi njegovega zastopnika, imenovanega v skladu s tretjim odstavkom prejšnjega člena,

5. države članice Evropske unije, 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 predložijo nemudoma ali najpozneje v treh mesecih od datuma spremembe informacij.

(3) Subjekti iz prvega odstavka tega člena predložijo informacije iz prvega in drugega odstavka tega člena pristojnemu nacionalnemu organu prek mehanizma za samoregistracijo zavezancev iz prvega odstavka 8. člena tega zakona.

(4) Pristojni nacionalni organ v vlogi enotne kontaktne točke po prejemu informacij iz prvega in drugega odstavka tega člena, razen informacij iz 6. točke prvega odstavka tega člena, te informacije nemudoma predloži agenciji ENISA.

33. člen

(podatkovna zbirka o registraciji domenskih imen)

(1) Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, za zagotovitev varnosti, stabilnosti in odpornosti DNS z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v zbirki podatkov.

(2) Zbirka podatkov iz prejšnjega odstavka mora vsebovati informacije o registraciji domenskih imen, ki zajemajo 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 in

– kontaktni elektronski naslov in telefonsko številko kontaktne točke, ki upravlja domensko ime, če se razlikuje od naslova imetnika domenskega imena.

Subjekti iz prvega odstavka tega člena morajo informacije iz tega odstavka po izbrisu iz zbirke podatkov hraniti ločeno še deset let po preteku koledarskega leta, v katerem so bili izbrisani iz zbirke podatkov, po preteku tega roka pa se izbrišejo oziroma uničijo tudi ločeno hranjene informacije.

(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 vsebujejo točne in popolne informacije, pri čemer se v politiki in postopkih upošteva, da morajo preveriti po vsaj en kontaktni podatek iz tretje in četrte alineje prejšnjega odstavka in določiti obdobja preverbe. Te politike in postopki morajo biti javno dostopni.

(4) Subjekti iz prvega odstavka tega člena po registraciji domenskega imena nemudoma omogočijo javno dostopnost podatkov o registraciji, ki niso osebni podatki. Takšne podatke objavijo na svojem spletnem mestu ali objavijo povezavo do spletnega mesta, kjer so ti podatki dostopni.

(5) Subjekti iz prvega odstavka tega člena nemudoma, najkasneje pa v 72 urah od prejema zakonitega in utemeljenega zahtevka osebe, ki ima upravičen razlog za dostop, omogočijo dostop do podatkov o registraciji posameznih domenskih imen. Politike in postopki v zvezi z razkritjem teh podatkov morajo biti javno dostopni.

(6) Izpolnjevanje obveznosti iz 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, med seboj sodelovati z izmenjavo relevantnih informacij.

VI. IZMENJAVA INFORMACIJ

34. člen

(dogovori o izmenjavi informacij o kibernetski varnosti)

(1) Zavezanci na podlagi tega zakona in 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 ali

– 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 s spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

(2) Izmenjava informacij iz prejšnjega odstavka poteka v sektorskih ali medsektorskih skupnostih zavezancev, lahko pa tudi 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. Podatki, ki so predmet izmenjave, morajo biti ustrezno označeni s semaforskim protokolom. Pri sklenitvi dogovorov o izmenjavi informacij se upoštevajo dobre prakse in smernice agencije ENISA.

(3) Dogovori o izmenjavi informacij o kibernetski varnosti iz prejšnjega odstavka vsebujejo vsebine in pogoje za takšne dogovore ter lahko vključujejo tudi operativne elemente, vključno glede uporabe namenskih digitalnih platform in orodij za avtomatizacijo. Pristojni nacionalni organ spodbuja sklenitev takšnih dogovorov z ozaveščanjem zavezancev in z metodološko podporo pri sklenitvi dogovorov.

(4) Bistveni in pomembni subjekti morajo pristojni nacionalni organ in za njih pristojno skupino CSIRT obvestiti o svojem sodelovanju pri dogovorih o izmenjavi informacij o kibernetski varnosti iz drugega odstavka tega člena, in to po sklenitvi takih dogovorov ali o odstopu od dogovora, ko odstop začne veljati. Skrbnik takšnega dogovora pošlje obvestilo pristojnemu nacionalnemu organu in pristojni skupini CSIRT v 15 dneh od nastanka dogodka.

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

35. člen

(prostovoljna priglasitev)

(1) Zavezanci lahko poleg obvezne priglasitve iz 30. člena tega zakona pristojni skupini CSIRT prostovoljno priglasijo incidente, kibernetske grožnje in skorajšnje incidente in jim predložijo ustrezne informacije.

(2) Subjekti, ki niso zavezanci po tem zakonu, lahko, ne glede na to, ali spadajo na področje uporabe tega zakona, skupini CSIRT iz prvega odstavka 13. člena tega zakona prostovoljno priglasijo pomembne incidente, kibernetske grožnje in skorajšnje incidente in ji predložijo ustrezne informacije.

(3) Prostovoljno priglasitev iz prvega in drugega odstavka tega člena skupine CSIRT obravnavajo v skladu s postopkom iz 30. člena tega zakona. Pri prostovoljnem poročanju za priglasitveni subjekt ne nastanejo dodatne obveznosti.

(4) Pristojne skupine CSIRT po potrebi informacije o priglasitvah, prejetih v skladu s tem členom, pošljejo pristojnemu nacionalnemu organu v vlogi enotne kontaktne točke, pri čemer poskrbijo za zaupnost in ustrezno varstvo informacij, ki jih je poslal priglasitveni subjekt.

(5) Pristojne skupine CSIRT lahko pred prostovoljnimi priglasitvami prednostno obravnavajo obvezne priglasitve. Pri določanju vrstnega reda obdelave prostovoljnih priglasitev upoštevajo vpliv prostovoljno priglašenih incidentov na neprekinjeno izvajanje storitev zavezanih subjektov in morebitni čezmejni vpliv.

(6) Prostovoljne priglasitve, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje storitev zavezancev in imajo zanemarljiv čezmejni vpliv, se obdelajo le, kadar takšna obdelava skupinam 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 30. člena tega zakona, po kateri poteka tudi izmenjava informacij med sodelujočimi organi na podlagi drugega odstavka 18. člena tega zakona. Sodelujoči organi imajo dostop do informacij o priglasitvah subjektov, ki so povezane z njihovim področjem dela.

VII. VREDNOTENJE INCIDENTA, OCENA OGROŽENOSTI IN UKREPANJE

36. člen

(vrednotenje incidenta in ukrepanje)

(1) Priglašene incidente ob njihovem reševanju vrednoti pristojna skupina CSIRT, ki poleg določb tega člena pri tem upošteva tudi nacionalni načrt odzivanja iz drugega odstavka 12. člena tega zakona. Če ima organ državne uprave zagotovljene zmogljivosti vsaj na ravni varnostno-operativnega centra, pristojna skupina CSIRT opravi vrednotenje po predhodnem posvetu z varnostno-operativnim centrom organa državne uprave. Če pristojni nacionalni organ ugotovi, da ocena pristojne skupine CSIRT ne izraža realnega stanja ali so bila ugotovljena nova dejstva, lahko incident prevrednoti. Varnostni dogodki in incidenti se vrednotijo v naslednje stopnje s poimenovanjem:

1. C6 dogodek # zaznane kibernetske aktivnosti, ki nimajo negativnega vpliva na omrežja in informacijske sisteme ali informacijske storitve zavezancev. Zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci;

2. C5 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 preprečilo, da bi se ta dogodek uresničil, ali se ni uresničil;

3. 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. Takšen incident ne sme imeti negativnega medsektorskega vpliva ali negativnega vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja;

4. C3 težji incident # enkraten pomemben incident ali zaporedje več 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 vpliv ali negativen vpliv na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja;

5. C2 težji incident # enkraten pomemben incident ali zaporedje več različnih incidentov v kratkem obdobju, kadar obstaja možnost, da preraste v kritični incident, in

6. C1 kritični incident # pomemben incident, ki poleg vplivov iz 4. točke tega odstavka povzroči tudi oteženo delovanje države, še posebej izvajanje nalog obrambe, notranje varnosti ter zaščite in reševanja, ali delno onemogoči delovanje vsaj treh visoko kritičnih sektorjev iz Priloge 1 ali enega v celoti.

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

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

(4) Pristojni nacionalni organ o težjih kibernetskih incidentih C3 in C2 obvešča osrednji organ za odzivanje na hibridne grožnje.

(5) Pristojni nacionalni organ lahko zavezancu v primeru težjega incidenta C3 ali C2 ali kritičnega incidenta C1 s pisno odločbo določi takšne primerne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic. V nujnih primerih, ko bi izdaja pisne odločbe zaradi poteka časa lahko negativno vplivala na učinkovitost takšnih ukrepov, lahko pristojni nacionalni organ zavezancu določi zadevne ukrepe tudi z ustno odločbo. V tem primeru se zavezancu pisni odpravek ustne odločbe vroči najpozneje v 48 urah po ustni odločbi.

(6) Če pristojna skupina CSIRT presodi, da nima vseh nujno potrebnih dejstev za opredelitev incidenta in za preprečitev nadaljnjih škodljivih posledic takšnega incidenta, za ugotovitev dejanskega stanja od zavezanca s pisnim pozivom zahteva podatke in pojasnila ali v nujnih primerih z ustnim pozivom, ko bi pisni poziv zaradi poteka časa lahko negativno vplival na učinkovitost reševanja zadevnega incidenta. Pri tem pristojna skupina CSIRT določi tudi rok za predložitev takšnih podatkov in pojasnil.

(7) Če zavezanec v postavljenem roku iz prejšnjega odstavka pristojni skupini CSIRT ne pošlje zahtevanih podatkov in pojasnil, lahko pristojni nacionalni organ na predlog pristojne skupine CSIRT s pisno odločbo zahteva predložitev podatkov in pojasnil ter določi rok za njihovo predložitev. V nujnih primerih, ko bi izdaja pisne odločbe zaradi poteka časa lahko negativno vplivala na učinkovitost reševanja zadevnega incidenta, lahko pristojni nacionalni organi o tem odloči tudi z ustno odločbo. V tem primeru se zavezancu pisni odpravek ustne odločbe vroči najpozneje v 48 urah po ustni odločbi.

(8) Ukrepi, izdani na podlagi petega, šestega in sedmega odstavka tega člena, se določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz petega odstavka tega člena. Podatki in informacije, zahtevani na podlagi prejšnjega odstavka, se zahtevajo v obsegu in roku, kot je to nujno potrebno za dosego namena iz prejšnjega odstavka. Zoper odločbi iz četrtega in sedmega odstavka tega člena ni dovoljena pritožba, dovoljen pa je upravni spor.

(9) Pristojni nacionalni organ lahko za preprečitev nastanka krize ali za njeno obvladovanje ali za hitrejše obvladovanje razmer in omejevanje nadaljnjih škodljivih posledic težjega incidenta C2 ali kritičnega incidenta C1 izda pisno odredbo, s katero pri zavezancih

odredi izvedbo nujnih ukrepov. Pri tem določi zlasti vrsto in obseg del, ki jih je treba opraviti pri zavezancu, ter rok za njihovo izvedbo. V nujnih primerih, ko bi izdaja pisne odredbe zaradi poteka časa lahko negativno vplivala na preprečitev nastanka krize ali njenega obvladovanja, lahko pristojni nacionalni organ o tem odloči tudi z ustno odredbo. V tem primeru se zavezancu pisni odpravek ustne odredbe vroči najpozneje v 48 urah po ustni odredbi.

(10) Pristojni nacionalni organ o ukrepih iz petega in osmega odstavka tega člena obvesti vlado in SNAV ter osrednji organ za odzivanje na hibridne grožnje.

37. člen

(ocena ogroženosti)

(1) Pristojni nacionalni organ izdela na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, oceno ogroženosti kibernetske varnosti v Republiki Sloveniji (v nadaljnjem besedilu: ocena ogroženosti). Za izdelavo ocene ogroženosti od organov, ki spadajo med ključne dele nacionalnega varnostnega sistema, na podlagi zaprosila pridobi tudi druge podatke, ki bi lahko vplivali na to oceno ogroženosti, in sicer v obsegu, kot je to nujno potrebno za izdelavo ocene ogroženosti. Pristojni nacionalni organ oceno ogroženosti preverja in po potrebi posodablja mesečno ali ob nenadni spremembi varnostnih razmer tudi prej. Pri tem ogroženost vrednoti kot:

– nizka ogroženost,

– srednja ogroženost,

– visoka ogroženost,

– kritična ogroženost.

(2) Ne glede na oceno ogroženosti iz prejšnjega odstavka zavezanci izvajajo najmanj ukrepe iz 21. in 22. člena tega zakona.

(3) Če 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 na svojem spletnem mestu in v sredstvih javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe.

(4) Kadar je ocena ogroženosti ovrednotena kot kritična, pristojni nacionalni organ o tem nemudoma obvesti vlado, SNAV in osrednji organ za odzivanje na hibridne grožnje, lahko pa jih glede na presojo relevantnih okoliščin in informacij obvesti tudi, kadar je ogroženost ovrednotena kot visoka. O oceni ogroženosti visoka ali kritična pristojni nacionalni organ obvesti zavezance, lahko pa obvesti tudi splošno javnost na svojem spletnem mestu in v sredstvih javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe. Pristojni nacionalni organ o preklicu ali spremembi ocene ogroženosti kritična ali visoka obvesti predhodno obveščene deležnike iz tega odstavka.

(5) V primerih ocene visoke ogroženosti morajo zavezanci nemudoma začeti izvajati vsaj naslednje dodatne varnostne ukrepe in jih izvajajo do preklica takšne ogroženosti:

– spremljanje varnostnih obvestil pristojne skupine CSIRT ali pristojnega nacionalnega organa, ki se nanašajo na razglašeno ogroženost visoka,

– preverjanje ustreznega ohranjanja dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja,

– takojšnje izvajanje varnostnih navodil skupine CSIRT ali pristojnega nacionalnega organa, ki se nanašajo na razglašeno ogroženost visoka, in

– poročanje o stanju varnosti svojih omrežij in informacijskih sistemov in o izvajanju ukrepov na način, kot to izhaja iz varnostnega navodila iz prejšnje alineje.

(6) V primerih ocene kritične ogroženosti morajo zavezanci poleg ukrepov iz prejšnjega odstavka nemudoma začeti izvajati tudi naslednje dodatne varnostne ukrepe in jih izvajajo do preklica takšne ogroženosti:

1. stalno spremljanje varnostnih obvestil pristojne skupine CSIRT ali pristojnega nacionalnega organa, ki se nanašajo na razglašeno kritično ogroženost,

2. preverjanje ustreznega delovanja beleženja in ohranjanja dnevniških zapisov iz 24. člena tega zakona ter poročanje o tem in morebitnih izvedenih aktivnostih v skladu s 6. točko tega odstavka,

3. spremljanje celotnega prometa na svojem omrežju za ugotavljanje anomalij in poročanje o tem ter morebitnih izvedenih aktivnostih v skladu s 6. točko tega odstavka,

4. takojšnje izvajanje morebitnih varnostnih navodil skupine CSIRT ali pristojnega nacionalnega organa, ki se nanašajo na razglašeno kritično ogroženost,

5. takojšnja priglasitev incidentov ne glede na roke iz 30. člena tega zakona,

6. vsaj tedensko poročanje pristojni skupini CSIRT o stanju varnosti svojih omrežij in informacijskih sistemov, tudi glede zaznav varnostnih dogodkov in s tem povezanih aktivnosti, ter o izvajanju varnostnih navodil iz 1. točke tega odstavka in

7. pogostejše poročanje pristojni skupini CSIRT o vsebinah iz prejšnje točke, če tako izhaja iz varnostnega navodila iz 1. točke tega odstavka.

(7) Ne glede na peti in šesti odstavek tega člena lahko pristojni nacionalni organ zavezancu s pisno odločbo določi takšne primerne in sorazmerne ukrepe, kot je to nujno potrebno za zmanjšanje ogroženosti. V nujnih primerih, ko bi lahko izdaja pisne odločbe zaradi poteka časa negativno vplivala na učinkovitost ukrepov za zmanjšanje ogroženosti, lahko pristojni nacionalni organ zavezancu določi zadevne ukrepe tudi z ustno odločbo. V tem primeru se zavezancu pisni odpravek ustne odločbe vroči najpozneje v 48 urah po ustni odločbi.

(8) Ukrepi, izdani na podlagi prejšnjega odstavka, se določijo v takšnem obsegu in za toliko časa, kot je to nujno potrebno za dosego namena iz prejšnjega odstavka. Zoper odločbo iz prejšnjega odstavka ni dovoljena pritožba, dovoljen pa je upravni spor.

(9) Pristojni nacionalni organ lahko za nižanje ocene visoke ali kritične ogroženosti ter posledično zaradi preprečitve nastanka krize ali njenega obvladovanja izda pisno odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih, varnostno-operativnih centrih organov državne uprave ali pri skupinah CSIRT. V odredbi se navedejo zlasti vrsta in obseg del, ki jih je treba opraviti pri prej navedenih subjektih, ter rok za njihovo izvedbo. Če bi lahko izdaja pisne odredbe zaradi poteka časa negativno vplivala na učinkovitost ukrepov za nižanje zadevne ocene ogroženosti, lahko pristojni nacionalni organ o tem odloči tudi z ustno odredbo. V tem primeru se zavezancu pisni odpravek ustne odredbe vroči najpozneje v 48 urah po ustni odredbi.

(10) Pristojni nacionalni organ o ukrepih iz sedmega in devetega odstavka tega člena obvesti vlado in SNAV ter osrednji organ za odzivanje na hibridne grožnje.

VIII. KIBERNETSKA OBRAMBA

38. člen

(kibernetska obramba)

Za preprečevanje kibernetskih groženj in incidentov v kibernetskem prostoru in za ublažitev njihovih vplivov se izvaja kibernetska obramba, ki 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 in njihove virtualne identitete,

– logično-tehnična plast zajema digitalne podatke iz tretje alineje 31. točke 5. člena tega zakona in

– fizična plast zajema omrežja in naprave iz prve in druge alineje 31. točke 5. člena tega zakona.

39. 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 in drugi državni 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 v skladu s svojimi pristojnostmi. Koordinacijo kibernetske obrambe na ravni državnih organov izvaja pristojni nacionalni organ, ki v ta namen vzpostavi koordinacijsko skupino.

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

– stalno zagotavljanje razpoložljivosti svojih komunikacijskih kanalov,

– prostori in podporni informacijski sistemi so na varnih krajih,

– zagotovijo zaupnost in zanesljivost svojih dejavnosti,

– imajo dovolj osebja za zagotavljanje neprekinjene razpoložljivosti storitev, pri čemer zagotavljajo, da je to osebje ustrezno usposobljeno, in

– imajo nadomestne 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 Slovenska obveščevalno-varnostna agencija stalno spremljajo stanje in odzive na dogodke v kibernetskem prostoru na področju svojega delovanja.

(4) Pristojni nacionalni organ za izvajanje 2. točke drugega odstavka 10. člena tega zakona za zgodnje zaznavanje kibernetskih groženj vzpostavi situacijski center kibernetske obrambe, ki je namenjen zaznavanju in spremljanju kibernetskih groženj ter izvajanju postopkov za zamejitev posledic kibernetskih groženj. Nosilci obrambnega načrtovanja, ki so določeni na podlagi zakona, ki ureja obrambo, se lahko vključijo v situacijski center kibernetske obrambe, ki v primeru njihove vključitve pristojnemu nacionalnemu organu omogoči neposreden, nujen in sorazmeren vpogled v delovanje njihovega omrežnega in informacijskega sistema. Situacijski center kibernetske obrambe deluje kot notranja organizacijska enota pristojnega nacionalnega organa.

(5) Pristojni nacionalni organ lahko zmogljivost situacijskega centra kibernetske obrambe ponudi tudi bistvenim in pomembnim subjektom, ki niso nosilci obrambnega načrtovanja iz prejšnjega odstavka. Pri tem vključeni subjekti za zgodnje zaznavanje kibernetskih groženj omogočijo pristojnemu nacionalnemu organu neposreden, nujen in sorazmeren vpogled v delovanje svojega omrežnega in informacijskega sistema.

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

(7) Izvajanje kibernetske obrambe iz prvega odstavka tega člena se dopolnjuje z vključevanjem organov in skupin CSIRT iz tega člena v mednarodne povezave in njihovim aktivnim sodelovanjem v teh povezavah ter z drugimi oblikami večstranskega in dvostranskega sodelovanja.

(8) Varnostno-operativni centri organov državne uprave pristojnemu nacionalnemu organu predložijo tedensko in letno poročilo o izvajanju svojih nalog. Poročilo obsega informacijo o pomembnih incidentih, ki so jih priglasili pristojni skupini CSIRT, in o drugih incidentih, ki so jih zaznali.

40. člen

(sodelovanje na področju kibernetske obrambe)

(1) Za kibernetsko obrambo lahko pristojni nacionalni organ sodeluje s subjekti javne uprave, gospodarstva, z raziskovalno-razvojnimi organizacijami, znanstvenimi institucijami, interesnimi združenji in posamezniki.

(2) Pristojni nacionalni organ lahko za izvajanje kibernetske obrambe k sodelovanju povabi tudi posameznike:

– ki so državljani Republike Slovenije,

– ki niso s pravnomočno odločbo postavljeni pod skrbništvo,

– ki so stari najmanj 18 let,

– ki niso pravnomočno obsojeni zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, in niso obsojeni na nepogojno kazen zapora v trajanju več kot šest mesecev

oziroma niso 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; v nadaljnjem besedilu KZ-1),

– zoper katere ni vložena pravnomočna obtožnica zaradi naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, oziroma ni bil uveden kazenski postopek zaradi suma storitve kaznivega dejanja iz 221. in 237. člena KZ-1,

– imajo soglasje delodajalca, če so v delovnem razmerju,

– imajo ustrezna znanja in kompetence za izvajanje nalog s področja informacijske in kibernetske varnosti ter

– se strinjajo s psihološkim testiranjem in varnostnim preverjanjem po 99. členu Zakona o nalogah in pooblastilih policije (Uradni list RS, št. 15/13, 23/15 – popr., 10/17, 46/19 – odl. US, 47/19 in 153/21 – odl. US).

(3) Pristojni nacionalni organ povabilo k sodelovanju iz prejšnjega odstavka objavi na osrednjem spletnem mestu državne uprave.

(4) Pristojni nacionalni organ opravi izbor kandidatov za sodelovanje pri kibernetski obrambi iz drugega odstavka tega člena ter zanje začne postopka psihološkega testiranja in varnostnega preverjanja iz zadnje alineje drugega odstavka tega člena. Po uspešno opravljenem varnostnem preverjanju jih uvrstitvi na seznam posameznikov, ki sodelujejo pri kibernetski obrambi. Ta seznam vsebuje:

– ime, priimek in rojstne podatke,

– davčno številko,

– naziv, naslov, telefonsko številko in elektronski naslov,

– doseženo izobrazbo,

– morebitno zaposlitev in

– znanja in kompetence.

(5) Pristojni nacionalni organ ponudi posamezniku s seznama iz prejšnjega odstavka sklenitev pogodbenega razmerja, v katerem se uredijo vrsta oziroma oblika pogodbenega razmerja, medsebojne pravice in dolžnosti ter nagrada. Če je posameznik v delovnem razmerju, se za ureditev njegovih pravic in dolžnosti upoštevajo določbe o dopolnilnem delu iz zakona, ki ureja delovna razmerja. Pristojni nacionalni organ po sklenitvi pogodbenega razmerja za posameznika organizira priprave, dodatna usposabljanja in vaje za delovanje na področju kibernetske obrambe.

(6) Pristojni nacionalni organ glede na potrebe in stanje ogroženosti kibernetske varnosti oblikuje eno ali več operativnih skupin za kibernetsko obrambo, v katere vključi posameznike, s katerimi ima sklenjeno pogodbo iz prejšnjega odstavka, in predstavnike državnih organov, organov lokalne samouprave, gospodarskih družb, zavodov in drugih organizacij iz prvega odstavka tega člena, ki so varnostno preverjeni, kot to določa osma alineja drugega odstavka tega člena. Pri oblikovanju operativnih skupin se upoštevajo tudi morebitna nasprotja interesov posameznikov do zavezancev.

(7) Direktor pristojnega nacionalnega organa imenuje vodjo in namestnika posamezne operativne skupine iz prejšnjega odstavka. Kadar 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.

(8) Sodelovanje javnih uslužbencev v operativni skupini iz šestega in sedmega odstavka tega člena je v interesu delodajalca v skladu z določbami o opravljanju dodatnega dela v interesu delodajalca iz zakona, ki ureja javne uslužbence.

41. člen

(dodatna 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, ter v primeru kibernetskih incidentov velikih razsežnosti ali kriz.

(2) Zavezanec ali pristojna skupina CSIRT lahko pristojni nacionalni organ zaprosi 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 in možnosti vključitve operativnih skupin iz prejšnjega člena se uskladijo pristojni nacionalni organ, pristojna skupina CSIRT in zavezanec, pri čemer upoštevajo tudi pravila, ki jih določa nacionalni načrt odzivanja.

(3) Če pomoč iz prejšnjega odstavka ni odobrena, pristojni nacionalni organ s tem seznani prosilca iz prejšnjega odstavka, ki lahko v primeru spremenjenih okoliščin znova zaprosi za pomoč.

42. člen

(pomoč pri kibernetski obrambi v Evropski uniji)

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

(2) Če pristojni nacionalni organ za obvladovanje stanja ali dogodkov iz prvega odstavka prejšnjega člena presodi, 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 pošlje vladi v odločanje. Medsebojni dogovor o pomoči določi tudi kritje morebitnih stroškov obeh strani, pri čemer morebitne stroške 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 pošlje v odločanje vladi. Pri odzivu na zaprosilo se upoštevata razpoložljivost zmogljivosti za kibernetsko obrambo in

aktualna ocena kibernetske varnosti v državi. Medsebojni dogovor o pomoči določi tudi kritje stroškov obeh strani, pri čemer stroške Republike Slovenije zagotovi organ, iz katerega izhaja napotena oseba.

43. člen

(pomoč pri kibernetski obrambi na mednarodni ravni)

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

(2) Za nudenje in prejem pomoči se smiselno uporablja prejšnji člen.

(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.

44. člen

(delo v manj ugodnem delovnem času)

(1) Uslužbenci organov, ki izvajajo kibernetsko obrambo, morajo opravljati delo tudi v manj ugodnem delovnem času, kadar je to potrebno za izvajanje s tem zakonom določenih nalog, če to terjajo varnostne razmere ali če je samo tako mogoče opraviti določene naloge, ki jih ni mogoče odlagati ali morajo biti opravljene v določenem roku. Delo v manj ugodnem delovnem času odredi predstojnik organa.

(2) Delo v manj ugodnem delovnem času je:

1. delo v neenakomerno razporejenem delovnem času,

2. delo v izmenah,

3. delo ob sobotah, nedeljah, praznikih in drugih dela prostih dnevih,

4. delo prek polnega delovnega časa,

5. popoldansko in nočno delo in

6. delo v deljenem delovnem času.

(3) Delo v manj ugodnem delovnem času se izvaja s prerazporeditvijo delovnega časa v okviru določene redne mesečne ali letne delovne obveznosti razen v primeru dela preko polnega delovnega časa.

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

(5) Ne glede na drugi do četrti odstavek tega člena se za delo v manj ugodnem delovnem času:

– na Ministrstvu za obrambo in v Slovenski vojski uporabljajo določbe, ki urejajo delo v manj ugodnih delovnih pogojih in v manj ugodnem delovnem času v zakonu, ki ureja obrambo, in v zakonu, ki ureja službo v Slovenski vojski,

– v Policiji uporabljajo določbe, ki urejajo delo v manj ugodnih delovnih pogojih in v manj ugodnem delovnem času v zakonu, ki ureja organiziranost in delo v Policiji,

– v Slovenski obveščevalno-varnostni agenciji uporabljajo določbe, ki urejajo delo v manj ugodnih delovnih pogojih in v manj ugodnem delovnem času v zakonu, ki ureja delovanje Slovenske obveščevalno-varnostne agencije, in

– v Upravi Republike Slovenije za zaščito in reševanje uporabljajo določbe, ki urejajo delo v manj ugodnih delovnih pogojih in v manj ugodnem delovnem času v zakonu, ki ureja varstvo pred naravnimi in drugimi nesrečami.

IX. NADZOR

45. člen

(splošne določbe)

(1) Za nadzor nad izvajanjem določb tega zakona, na njegovi podlagi sprejetih predpisov in nad izvršitvijo upravnih odločb, izdanih na podlagi petega ali sedmega odstavka 36. člena, sedmega odstavka 37. člena tega zakona, nad izvršitvijo odredb, izdanih na podlagi devetega odstavka 36. člena in devetega odstavka 37. člena tega zakona, so pristojni inšpektorji za informacijsko varnost pristojnega nacionalnega organa (v nadaljnjem besedilu: inšpektor), razen na obrambnem področju, kjer ta nadzor izvaja Inšpektorat Republike Slovenije za obrambo ter na področju obveščevalno-varnostne dejavnosti, kjer ta nadzor izvaja Inšpektorat Republike Slovenije za notranje zadeve.

(2) Inšpektor je pristojen tudi za nadzor nad izvajanjem določb Uredbe 2019/881/EU in izvajanjem evropskih certifikacijskih shem ter nad izvršitvijo upravnih odločb, ki jih nacionalni certifikacijski organ za kibernetsko varnost izda na podlagi sedmega ali osmega odstavka 27. člena tega zakona.

(3) Inšpektor nadzira tudi izvajanje izvedbenih aktov Evropske komisije, sprejetih na podlagi Direktive 2022/2555/EU, ki imajo neposredni učinek v pravnem redu Republike Slovenije.

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

(5) Pri opravljanju nalog inšpekcijskega nadzora pri zavezancu iz tega zakona ima inšpektor poleg pravic iz zakona, ki ureja inšpekcijski nadzor, tudi naslednja pooblastila:

1. opraviti inšpekcijski pregled na kraju samem in nadzor na daljavo, ki ju lahko izvede skupaj z usposobljenimi strokovnjaki;

2. opraviti inšpekcijski varnostni pregled, ki temelji na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganj;

3. opraviti neposreden vpogled v podatke, dokumentacijo ter v omrežne in informacijske sisteme;

4. preveriti pogoje in način izvajanja ukrepov za obvladovanje tveganj kibernetske varnosti;

5. pregledati območja, objekte in prostore zavezancev, kjer so ključni, krmilni in nadzorni informacijski sistemi in podatki;

6. pregledati dokumentacijo o izvrševanju predpisanih obveznosti obveščanja o kibernetskih incidentih in drugih obveznostih na podlagi zahtev pristojnih organov iz tega zakona;

7. pregledati poročila o izvedbi revizije informacijskih sistemov ter izvedbi varnostnih pregledov omrežja in informacijskih sistemov in

8. pregledati drugo dokumentacijo, potrebno za izvedbo nadzora.

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

(7) Zoper odločbo, izdano v postopkih nadzora po tem zakonu, ni dovoljena pritožba, dovoljen pa je upravni spor.

(8) 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.

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

46. člen

(nadzor bistvenih subjektov)

(1) Inšpektor lahko pri izvajanju svojih nadzornih nalog pri bistvenih subjektih izvaja naključne inšpekcijske nadzore.

(2) Če inšpektor pri opravljanju nalog inšpekcijskega nadzora ugotovi, da je bistveni subjekt kršil ta zakon, drug predpis ali drug akt, katerega izvajanje nadzoruje, ima poleg pravic in dolžnosti iz zakona, ki ureja inšpekcijski nadzor, tudi pravico in dolžnost:

1. odrediti izvedbo redne in ciljno usmerjene revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti, ki jo izvede revizor informacijskih sistemov;

2. odrediti izvedbo izredne revizije skladnosti, ki jo izvede revizor informacijskih sistemov, ko je to utemeljeno zaradi pomembnega incidenta ali ker je bistveni subjekt očitno kršil ta zakon;

3. zavezancu odrediti, da obvesti fizične ali pravne osebe, v zvezi s katerimi opravlja storitve ali izvaja dejavnost in na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje in o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;

4. odrediti, da zavezanec v razumnem roku izvede priporočila, dana na podlagi izvedene revizije skladnosti;

5. imenovati pooblaščeno osebo z natančno opredeljenimi nalogami v določenem obdobju, ki spremlja, ali bistveni subjekt izpolnjuje 21., 22., 29. in 30. člen tega zakona, in

6. zavezancu odrediti, da na določen način objavi kršitve tega zakona.

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

1. začasno prepove izvajanje dela storitev ali dejavnosti ali začasno prepove izvajanje vseh storitev ali dejavnosti, ki jih opravlja bistveni subjekt, in

2. zahteva začasno prepoved opravljanja vodstvenih funkcij vsem osebam, ki za bistveni subjekt opravljajo poslovodne naloge na ravni glavnega izvršnega direktorja ali pravnega zastopnika.

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

(5) Ukrepi iz tretjega odstavka tega člena se ne uporabljajo za subjekte javne uprave na državni ravni.

(6) Inšpektor pri sprejemanju ukrepov iz drugega in tretjega odstavka tega člena upošteva okoliščine vsakega posameznega primera, pri čemer ustrezno upošteva:

1. resnost kršitve in pomembnost kršenih določb, pri čemer se za resne kršitve v vsakem primeru štejejo:

   – ponavljajoče se kršitve,

   – nepriglasitev ali neodprava pomembnih incidentov,

   – neodprava pomanjkljivosti v skladu z zavezujočimi navodili inšpektorja,

   – oviranje revizij ali dejavnosti spremljanja, ki jih je odredil inšpektor po ugotovitvi kršitve,

   – predložitev napačnih informacij v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost ali obveznostmi poročanja iz 21., 22., 29. ali 30. 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. naklep ali malomarnost storilca kršitve;

6. ukrepe, ki jih je bistveni subjekt sprejel za preprečevanje ali zmanjšanje premoženjske ali nepremoženjske škode;

7. upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov certificiranja in

8. raven sodelovanja odgovornih fizičnih ali pravnih oseb z inšpektorjem.

(7) 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.

(8) Redne in ciljno usmerjene revizije skladnosti iz 1. točke drugega odstavka tega člena temeljijo na ocenah tveganj, ki jih izvedejo pristojni nacionalni organi ali bistveni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Poročilo o izvedeni ciljno usmerjeni reviziji varnosti se da na voljo inšpektorju.

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

(10) Inšpektor pri izvajanju svojih pooblastil navede namen zahteve in opredeli zahtevane informacije. Pri odreditvi izredne revizije skladnosti iz 2. točke drugega odstavka tega člena inšpektor določi obseg revizije.

(11) Kadar izvaja nadzor nad bistvenim subjektom, ki je na podlagi zakona, ki ureja kritično infrastrukturo, določen kot kritičen, inšpektor obvesti pristojno inšpekcijo za področje kritične infrastrukture. Inšpektor za področje kritične infrastrukture lahko Inšpekciji za informacijsko varnost tudi sam poda obrazloženo pobudo, da izvede nadzor v zvezi s subjektom, ki je na podlagi zakona, ki ureja kritično infrastrukturo, določen kot kritičen.

(12) Inšpektor sodeluje z nadzornimi organi, ki so določeni z zakonom, ki ureja izvajanje Uredbe 2022/2554/EU o digitalni operativni odpornosti za finančni sektor. Pri tem inšpektor zagotovi, da o nadzoru bistvenega subjekta, ki je imenovan za ključnega tretjega ponudnika storitev IKT na podlagi 31. člena Uredbe 2022/2554/EU, o tem obvesti nadzorniški forum, ustanovljen na podlagi prvega odstavka 32. člena Uredbe 2022/2554/EU.

(13) 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 eurov. Vsaka poznejša denarna kazen za prisilitev je lahko znova izrečena do tega zneska.

(14) Prejšnji odstavek se ne uporablja za pravne osebe javnega prava.

(15) Predstojnik organa subjekta javne uprave ali odgovorna oseba pravne osebe, ki je bistven subjekt, to je fizična oseba ali osebe, ki vodijo, nadzorujejo ali upravljajo poslovanje pravne osebe oziroma so po zakonu, aktu o ustanovitvi ali pooblastilu pristojne in dolžne zagotoviti zakonito delovanje, je odgovorna oseba za zagotavljanje skladnosti delovanja bistvenega subjekta po tem zakonu (v nadaljnjem besedilu: odgovorna oseba bistvenega subjekta) in odgovarja za kršitve svojih dolžnosti v skladu s tem zakonom.

47. 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, ali da ne izpolnjuje obveznosti v zvezi z obveščanjem o kibernetskih incidentih na predpisani način in v predpisanih rokih, ali da ne ravna po zahtevah pristojnega nacionalnega organa iz tega zakona.

(2) Če inšpektor pri opravljanju nalog inšpekcijskega nadzora ugotovi, da je pomembni subjekt kršil ta zakon ali drug predpis ali drug akt, katerega izvajanje nadzoruje, ima poleg pravic in dolžnosti iz zakona, ki ureja inšpekcijski nadzor, tudi pravico in dolžnost:

1. odrediti izvedbo ciljno usmerjene revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti, ki jo izvede revizor informacijskih sistemov,

2. odrediti, da zavezanec obvesti fizične ali pravne osebe, za katere opravlja storitve ali izvaja dejavnosti in na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje in o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe izvedejo v odziv na to grožnjo,

3. odrediti, da zavezanec v razumnem roku izvede priporočila, dana na podlagi ciljno usmerjene revizije skladnosti, in

4. odrediti, da zavezanec na določen način objavi kršitve tega zakona.

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

1. resnost kršitve in pomembnost kršenih določb, pri čemer se za resne kršitve med drugim v vsakem primeru štejejo:

   – ponavljajoče se kršitve,

   – nepriglasitev ali neodprava pomembnih incidentov,

   – neodprava pomanjkljivosti v skladu z zavezujočimi navodili inšpektorja,

   – oviranje revizij ali dejavnosti spremljanja, ki jih je inšpektor odredil po ugotovitvi kršitve,

   – predložitev napačnih informacij v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost ali obveznostmi poročanja iz 21., 22., 29. in 30. 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 in

8. raven sodelovanja odgovornih fizičnih ali pravnih oseb z inšpektorjem.

(4) Ciljno usmerjene revizije skladnosti iz 1. točke drugega odstavka tega člena temeljijo na ocenah tveganj, ki jih izvedejo pristojni nacionalni organi ali pomembni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Poročilo o izvedeni ciljno usmerjeni reviziji skladnosti se da na voljo inšpektorju.

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

(6) Predstojnik organa subjekta javne uprave ali odgovorna oseba pravne osebe, ki je pomembni subjekt, to je fizična oseba ali osebe, ki vodijo, nadzorujejo ali upravljajo poslovanje pravne osebe oziroma so po zakonu, aktu o ustanovitvi ali pooblastilu pristojne in dolžne zagotoviti zakonito delovanje, je odgovorna oseba za zagotavljanje skladnosti delovanja pomembnega subjekta po tem zakonu (v nadaljnjem besedilu: odgovorna oseba pomembnega subjekta) in odgovarja za kršitve svojih dolžnosti v skladu s tem zakonom.

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

(8) Prejšnji odstavek se ne uporablja za pravne osebe javnega prava.

(9) Inšpektor sodeluje z nadzornimi organi, ki so določeni z zakonom, ki ureja izvajanje Uredbe 2022/2554/EU o digitalni operativni odpornosti za finančni sektor. Pri tem inšpektor zagotovi, da o nadzoru pomembnega subjekta, ki je imenovan za ključnega tretjega ponudnika storitev IKT na podlagi 31. člena Uredbe 2022/2554/EU, o tem obvesti nadzorniški forum, ustanovljen na podlagi prvega odstavka 32. člena Uredbe 2022/2554/EU.

48. člen

(nadzor subjektov po Uredbi 2019/881/EU)

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

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

(3) Pri opravljanju nalog inšpekcijskega nadzora pri zavezancu iz Uredbe 2019/881/EU ima inšpektor poleg pravic iz zakona, ki ureja inšpekcijski nadzor, tudi pravico, da opravi inšpekcijski pregled na kraju samem in nadzor na daljavo, ki ju lahko izvede skupaj z usposobljenimi strokovnjaki.

(4) Če inšpektor pri opravljanju nalog inšpekcijskega nadzora ugotovi, da je zavezanec iz Uredbe 2019/881/EU kršil ta zakon ali drug predpis ali drug akt, katerega izvajanje nadzoruje, ima poleg pravic in dolžnosti iz zakona, ki ureja inšpekcijski nadzor, tudi pravico in dolžnost:

1. odrediti izvedbo ciljno usmerjene revizije skladnosti z Uredbo 2019/881/EU, ki jo izvede revizor informacijskih sistemov, in

2. odrediti izvedbo ustreznih ukrepov, da se zagotovi izpolnjevanje zahtev iz Uredbe 2019/881/EU ali evropske certifikacijske sheme.

(5) Inšpektor lahko nacionalnemu certifikacijskemu organu za kibernetsko varnost predlaga preklic evropskega certifikata kibernetske varnosti, kadar tak certifikat ni skladen z Uredbo 2019/881/EU ali z evropsko certifikacijsko shemo.

(6) Poročilo o izvedeni ciljno usmerjeni reviziji skladnosti iz 1. točke četrtega odstavka tega člena se predloži inšpektorju.

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

49. člen

(določitev revizorja informacijskih sistemov)

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

(2) Ne glede na prejšnji odstavek lahko bistveni ali pomembni subjekt, ki ima med svojimi zaposlenimi osebo, ki ima status aktivnega preizkušenega revizorja informacijskih sistemov, za zadevno revizijo izbere tudi to svojo zaposleno osebo, če lahko zagotovi nepristranskost in neodvisnost revizorja.

(3) Če bistveni ali pomembni subjekt ne izbere revizorja informacijskih sistemov v skladu s prvim ali drugim odstavkom tega člena, revizorja informacijskih sistemov s sklepom določi inšpektor.

50. člen

(kršitve, ki pomenijo kršitev varstva osebnih podatkov)

(1) Inšpektor o obravnavi zadev iz prvega odstavka 45. člena tega zakona, katerih posledica je kršitev varstva osebnih podatkov, obvesti Informacijskega pooblaščenca. Informacijskega pooblaščenca obvesti tudi v primerih suma kršitve varstva osebnih podatkov. O obravnavi takšnih zadev, ki se nanašajo na operaterje po zakonu, ki ureja elektronske komunikacije, inšpektor obvesti tudi Agencijo za komunikacijska omrežja in storitve Republike Slovenije.

(2) Kadar Informacijski pooblaščenec zaradi kršitve varstva osebnih podatkov iz prejšnjega odstavka naloži globo na podlagi zakona, ki ureja varstvo osebnih podatkov, inšpektor zaradi istega ravnanja ne naloži globe, lahko pa naloži ukrepe po tem zakonu.

(3) Kadar ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4. 5. 2016, str. 1), sedež v drugi državi članici Evropske unije kot inšpektor, inšpektor obvesti Informacijskega pooblaščenca o možni kršitvi varstva osebnih podatkov iz prvega odstavka tega člena.

51. člen

(medsebojna pomoč in čezmejni nadzor)

(1) Kadar bistveni ali pomembni subjekt spada v pristojnost pristojnega nacionalnega organa v skladu z 31. členom tega zakona, vendar opravlja storitve:

– v več kot eni državi članici Evropske unije ali

– v eni ali več državah članicah Evropske unije in so njegovi omrežni in informacijski sistemi v drugi državi članici Evropske unije ali v več kot eni državi članici Evropske unije,

lahko inšpektor 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 med seboj pomagajo pri izvajanju takega nadzora.

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

– obvešča pristojne organe nadzora v drugih državah članicah Evropske unije o svojih sprejetih nadzornih ukrepih in izrečenih ukrepih za odpravo nepravilnosti,

– lahko od pristojnega organa nadzora v drugi državi članici Evropske unije zahteva izvedbo nadzornih ukrepov ali izrek ukrepov za odpravo nepravilnosti in

– zahteva od pristojnega organa nadzora v drugi državi članici Evropske unije sorazmerno medsebojno pomoč ali mu na obrazloženo zahtevo zagotovi tako pomoč.

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

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

– ni pristojen za zagotavljanje zahtevane medsebojne pomoči,

– zahtevana medsebojna pomoč ni skladna s pristojnostmi inšpektorja po tem zakonu in

– 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 pristojnimi organi nadzora držav članic Evropske unije, ki so tudi pristojne za obravnavo nadzora v konkretnem primeru. Če druga država članica Evropske unije, v katere pristojnost tudi spada obravnava zadevnega postopka nadzora, tako zahteva, se mora inšpektor pred zavrnitvijo zahteve za medsebojno pomoč predhodno posvetovati tudi z Evropsko komisijo in agencijo 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.

X. KAZENSKE DOLOČBE

52. člen

(prekrški bistvenih subjektov)

(1) Z globo v višini od 0,5 odstotka do 2 odstotka skupnega letnega prometa pravne osebe, doseženega v preteklem poslovnem letu, vendar ne manj kot 10.000 eurov in ne več kot 10.000.000 eurov, odvisno od tega, kateri znesek je višji, se kaznuje pravna oseba, če:

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 21. člena tega zakona,

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega, šestega, sedmega, osmega, devetega, enajstega ali trinajstega odstavka 22. člena tega zakona,

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega, šestega, sedmega ali devetega odstavka 24. člena tega zakona,

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega, šestega in sedmega odstavka 29. člena tega zakona ali

– ne izpolni obveznosti iz prvega ali drugega odstavka 30. člena tega zakona.

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

(3) Z globo od 1.000 eurov do 10.000 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, če stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 3.000 eurov do 15.000 eurov se kaznuje pravna oseba, če:

1. ne izpolni obveznosti iz drugega ali petega odstavka 8. člena tega zakona,

2. ne izpolni obveznosti iz drugega, tretjega, četrtega ali petega odstavka 20. člena tega zakona,

3. ne izpolni obveznosti iz prvega ali drugega odstavka 25. člena tega zakona,

4. ne izpolni obveznosti iz prvega odstavka 26. člena tega zakona,

5. ne izpolni obveznosti iz šestnajstega odstavka 27. člena tega zakona,

6. ne izpolni obveznosti iz prvega odstavka 28. člena tega zakona,

7. ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 32. člena tega zakona,

8. ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega ali petega odstavka 33. člena tega zakona,

9. ne izpolni obveznosti iz petega ali šestega odstavka 37. člena tega zakona,

10. ne izpolni obveznosti iz odločbe, izdane na podlagi sedmega ali devetega odstavka 37. člena tega zakona, ali

11. ne izpolni obveznosti iz prvega odstavka 49. člena tega zakona.

(5) Z globo od 1.000 eurov do 10.000 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 eurov do 3.000 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 ali samoupravni lokalni skupnosti, če ne izpolni obveznosti iz četrtega odstavka tega člena.

53. člen

(prekrški pomembnih subjektov)

(1) Z globo v višini od 0,3 odstotka do 1,4 odstotka skupnega letnega prometa pravne osebe, doseženega v preteklem poslovnem letu, vendar ne manj kot 7.000 eurov in ne več kot 7.000.000 eurov, odvisno od tega, kateri znesek je višji, se kaznuje pravna oseba, če:

– ne izpolni obveznosti iz prvega, drugega, tretjega ali petega odstavka 21. člena tega zakona,

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega, šestega, sedmega, osmega, devetega ali trinajstega odstavka 22. člena tega zakona,

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, šestega, sedmega ali devetega odstavka 24. člena tega zakona,

– ne izpolni obveznosti iz prvega, drugega, tretjega, četrtega, petega, šestega ali sedmega odstavka 29. člena tega zakona ali

– ne izpolni obveznosti iz prvega ali drugega odstavka 30. člena tega zakona.

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

(3) Z globo od 1.000 eurov do 7.000 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, ki je pomemben subjekt po tem zakonu, če stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 1.000 eurov do 10.000 eurov, se kaznuje pravna oseba, če:

1. ne izpolni obveznosti iz drugega ali petega odstavka 8. člena tega zakona,

2. ne izpolni obveznosti iz drugega, tretjega, četrtega ali petega odstavka 20. člena tega zakona,

3. ne izpolni obveznosti iz tretjega, četrtega ali petega odstavka 25. člena tega zakona,

4. ne izpolni obveznosti iz prvega odstavka 26. člena tega zakona,

5. ne izpolni obveznosti iz šestnajstega odstavka 27. člena tega zakona,

6. ne izpolni obveznosti iz prvega odstavka 28. člena tega zakona,

7. ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 32. člena tega zakona,

8. ne izpolni obveznosti iz petega ali šestega odstavka 37. člena tega zakona,

9. ne izpolni obveznosti iz odločbe, izdane na podlagi sedmega ali devetega odstavka 37. člena tega zakona,

10. ne izpolni obveznosti iz prvega odstavka 49. člena tega zakona.

(5) Z globo od 500 eurov do 7.000 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 eurov do 2.000 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 ali v samoupravni lokalni skupnosti, če ne izpolni obveznosti iz četrtega odstavka tega člena.

54. člen

(prekrški upravljavca centralnega državnega informacijsko-komunikacijskega sistema)

Z globo od 200 eurov do 2.000 eurov se za prekršek kaznuje odgovorna oseba upravljavca centralnega državnega informacijsko-komunikacijskega sistema, če:

– pristojni skupini CSIRT iz prvega odstavka 13. člena tega zakona ne omogoči vpogleda v delovanje informacijske infrastrukture centralnega državnega informacijsko-komunikacijskega sistema (sedmi odstavek 15. člena),

– v svojem informacijsko-komunikacijskem sistemu ne izvede odrejenih ukrepov pristojne skupine CSIRT iz prvega odstavka 13. člena tega zakona (osmi odstavek 15. člena).

55. člen

(prekrški za kršitev Uredbe 2019/881/EU)

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

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

(3) Z globo od 500 eurov do 5.000 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, ki je proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT iz 53. člena Uredbe 2019/881/EU, če stori prekršek iz prvega odstavka tega člena.

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

– ne da na voljo dodatnih informacij o kibernetski varnosti iz prvega odstavka 55. člena Uredbe 2019/881/EU ali so te informacije nepopolne ali zavajajoče ali

– pred iztekom veljavnosti ustreznega evropskega certifikata kibernetske varnosti ali izjave EU o skladnosti v nasprotju z drugim odstavkom 55. člena Uredbe 2019/881/EU onemogoči dostop do dodatnih informacij o kibernetski varnosti ali informacij ne posodablja.

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

(6) Z globo od 500 eurov do 2.000 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 ali samoupravni lokalni skupnosti, ki je proizvajalec ali ponudnik certificiranih proizvodov, storitev in postopkov IKT ali proizvodov, storitev in postopkov IKT, za katere je bila izdana izjava EU o skladnosti iz 55. člena Uredbe 2019/881/EU, če stori prekršek iz četrtega odstavka tega člena.

56. člen

(odmerjanje sankcij za prekrške)

(1) Poleg splošnih pravil za odmero sankcije iz zakona, ki ureja prekrške, se pri odločanju o višini izrečene globe, če bistveni in pomembni subjekti kršijo 21., 22., 24., 29. ali 30. člen tega zakona, upošteva tudi letni promet ali letna bilančna vsota bistvenega ali pomembnega subjekta v predhodnem poslovnem letu.

(2) Pri odločanju o naložitvi in višini višine globe iz tega člena se upoštevajo okoliščine posameznega primera in elementi iz šestega odstavka 46. člena oziroma tretjega odstavka 47. člena tega zakona.

57. 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.

58. člen

(uporaba določb o prekrških)

Višina in razponi glob, ki so določeni v 52. in 53. členu tega zakona, veljajo in se uporabljajo ne glede na določbe zakona, ki ureja prekrške.

XI. PREHODNE DOLOČBE

59. člen

(skupine CSIRT)

Do določitve skupin CSIRT iz prvega odstavka 13. člena tega zakona njihove naloge izvajata:

– SIGOV-CERT, ki deluje kot notranja organizacijska enota pri pristojnem nacionalnem organu in je pristojen za obravnavo incidentov subjektov javne uprave na državni in lokalni ravni ter ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave, ter

– SI-CERT, ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije in je pristojen za obravnavo incidentov, ki jih priglasijo drugi zavezanci iz prvega odstavka 6. člena tega zakona, ki niso zajeti v prejšnji alineji, ter deluje kot koordinator iz prvega odstavka 17. člena tega zakona. Pristojen je tudi za obravnavo prostovoljno priglašenih incidentov subjektov, ki niso zavezanci po tem zakonu v skladu z drugim odstavkom 35. člena tega zakona.

60. člen

(vzpostavitev samoregistracije in seznamov ter obveščanje)

(1) Pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz 6. člena tega zakona po prvem odstavku 8. člena tega zakona v štirih mesecih od uveljavitve tega zakona.

(2) Zavezanci, ki ob uveljavitvi tega zakona izpolnjujejo merila iz 6. in 7. člena tega zakona, opravijo prvo registracijo po mehanizmu za samoregistracijo v šestih mesecih od uveljavitve tega zakona. Do vzpostavitve mehanizma za samoregistracijo se informacije pošljejo v digitalni obliki na elektronski naslov pristojnega nacionalnega organa.

(3) Organi iz sedmega odstavka 8. člena tega zakona prvič pošljejo poimenski seznam iz tega člena pristojnemu nacionalnemu organu v šestih mesecih od uveljavitve tega zakona.

(4) Pristojni nacionalni organ vzpostavi prvi seznam iz četrtega odstavka 8. člena tega zakona v enem mesecu po izteku roka iz prejšnjega odstavka.

(5) Vlada sprejme program usposabljanja odgovornih oseb iz šestega odstavka 20. člena tega zakona v šestih mesecih od uveljavitve tega zakona.

(6) Pristojni nacionalni organ vzpostavi namensko digitalno platformo iz desetega odstavka 30. člena tega zakona v enem letu od uveljavitve tega zakona. Do njene vzpostavitve zadevni subjekti priglasitve iz 29. in 35. člena tega zakona pošiljajo na elektronski naslov pristojne skupine CSIRT iz tega zakona. Do vzpostavitve te platforme tudi izmenjava informacij iz drugega odstavka 18. člena tega zakona poteka v digitalni obliki prek elektronskih naslovov pristojnega nacionalnega organa in sodelujočih organov.

(7) Subjekti iz prvega odstavka 32. člena tega zakona o informacijah iz navedene določbe prvič obvestijo pristojni nacionalni organ v šestih mesecih od uveljavitve tega zakona.

(8) Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, vzpostavijo politike in postopke iz tretjega in petega odstavka 33. člena tega zakona v šestih mesecih od uveljavitve tega zakona.

(9) Organi iz prvega odstavka 39. člena tega zakona obvestijo pristojni nacionalni organ o varnostno-operativnih centrih organov državne uprave, ki izpolnjujejo zahteve iz drugega odstavka 39. člena tega zakona, v tridesetih dneh od uveljavitve tega zakona.

(10) Organi iz prvega odstavka 39. člena tega zakona obvestijo pristojni nacionalni organ o varnostno-operativnih centrih organov državne uprave, ki ne izpolnjujejo zahtev iz drugega odstavka 39. člena tega zakona, v tridesetih dneh od uveljavitve tega zakona in zagotovijo izpolnjevanje teh v enem letu od uveljavitve zakona.

61. člen

(status izvajalcev bistvenih storitev in organov državne uprave)

Subjekti, ki so bili na podlagi drugega ali tretjega odstavka 6. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV) kot izvajalci bistvenih storitev določeni pred 16. januarjem 2023, in organi državne uprave, ki upravljajo informacijske sisteme in dele omrežja ali izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljnjem besedilu: organi državne uprave), in so bili kot zavezani organi državne uprave na podlagi prvega odstavka 9. člena ZInfV določeni pred uveljavitvijo tega zakona, so še naprej zavezani kot bistveni subjekti po tem zakonu.

62. člen

(sprejetje ukrepov za obvladovanje tveganj)

(1) Bistveni in pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz 21. in 22. člena tega zakona v osemnajstih mesecih od uveljavitve tega zakona.

(2) Ne glede na prejšnji odstavek bistveni subjekti, ki so bili določeni kot izvajalci bistvenih storitev na podlagi 6. člena ZInfV in organi državne uprave, ki so bili določeni na podlagi 9. člena ZInfV, sprejmejo ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz 21. in 22. člena tega zakona v enem letu od uveljavitve tega zakona. Do izteka tega roka se zanje uporabljajo varnostne zahteve, varnostna dokumentacija, varnostni ukrepi in pripadajoče določbe o nadzoru ter kazenske določbe iz ZInfV in predpisa iz druge ali tretje alineje drugega odstavka 69. člena tega zakona.

(3) Ne glede na prvi odstavek tega člena bistveni in pomembni subjekti, ki so operaterji po Zakonu o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O), sprejmejo ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz 21. in 22. člena tega zakona v enem letu od uveljavitve tega zakona. Do izteka tega roka se zanje uporabljajo varnostni ukrepi iz VII. poglavja Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) in splošni akt iz druge alineje tretjega odstavka 69. člena tega zakona.

63. člen

(uskladitev podatkovne zbirke o registraciji domenskih imen)

Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen, uskladijo podatkovne zbirke o registraciji domenskih imen z drugim in četrtim odstavkom 33. člena tega zakona za registracije, ki so bile izvedene do uveljavitve tega zakona, v osemnajstih mesecih od uveljavitve tega zakona.

64. člen

(izdaja podzakonskih predpisov in strategije)

(1) Vlada izda predpisa iz tretjega odstavka 4. člena in šestega odstavka 20. člena tega zakona v šestih mesecih 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 sprejme strategijo iz 9. člena tega zakona v enem letu od uveljavitve tega zakona.

(4) Vlada sprejme nacionalni načrt odzivanja iz tretjega odstavka 12. člena tega zakona v treh mesecih od uveljavitve tega zakona.

65. člen

(spremembe in dopolnitve Zakona o elektronskih komunikacijah)

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

1. se v 115. členu besedilo člena nadomesti z besedilom:

»(1) Operaterji morajo v skladu z zakonom, ki ureja informacijsko varnost, vzpostaviti in vzdrževati dokumentirana SUVI in SUNP ter pri tem sprejeti ustrezne, učinkovite in sorazmerne tehnične, operativne in organizacijske ukrepe za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter ukrepe za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve.

(2) Operater mora SUVI in SUNP določiti kot poslovno skrivnost.

(3) V delu, v katerem se SUNP iz prvega odstavka nanaša na zagotavljanje komunikacije v sili, mora biti ta pregledan vsaj enkrat letno. Za njegovo sprejetje in morebitne spremembe ali posodobitve je potrebna predhodna odobritev pristojnih organov, odgovornih za delovanje centrov za sprejem komunikacije v sili.

(4) Če iz dokumentov ali tehničnih priporočila agencije ENISA ter smernic Evropske komisije izhaja, da so zaradi zagotovitve višje ravni kibernetske varnosti ob upoštevanju varnostnih tveganj potrebni tudi sektorsko specifični ukrepi za operaterje, agencija izda splošni akt, s katerim predpiše posebne tehnične usmeritve ter tehnične in organizacijske ukrepe. Pri sprejetju splošnega akta agencija sodeluje z organom, pristojnim za informacijsko varnost.«;

2. se v 116. členu v četrtem odstavku v prvem stavku besedilo »iz tretjega odstavka prejšnjega člena« nadomesti z besedilom »v skladu s prejšnjim členom«;

3. se 118., 119., 120., 121. in 122. člen črtajo;

4. se v 123. členu v prvem odstavku za prvim stavkom doda besedilo, ki se glasi: »Revizija varnosti po tem zakonu ne vključuje primerov iz prvega odstavka 115. člena tega zakona, ki potekajo v skladu z zakonom, ki ureja informacijsko varnost. Agencija lahko pri zahtevi za revizijo in pregledu rezultatov revizije, ki jih zahteva, zaprosi za pomoč pristojni nacionalni organ iz zakona, ki ureja informacijsko varnost.«;

5. se v 124. členu v četrtem odstavku besedilo »se uporablja določba petega odstavka 115. člena tega zakona« nadomesti z besedilom »mora biti ta pregledan vsaj enkrat letno. Za njegovo sprejetje in spremembe ali posodobitve je potrebna predhodna odobritev pristojnih organov, odgovornih za delovanje centrov za sprejem komunikacije v sili.«;

6. se v 128. členu besedilo »določb 120. in 121.« nadomesti z besedilom »prvega odstavka 115.«, poleg tega se na koncu doda nov stavek, ki se glasi: »Agencija nadzira tudi izvajanje odločbe iz prvega odstavka 117. člena tega zakona«;

7. se v 287. členu v prvem odstavku v prvem stavku črta besedilo »ali organa, pristojnega za informacijsko varnost na podlagi 128. člena tega zakona«, besedilo tretjega stavka pa se nadomesti z besedilom »Agencija izvaja tudi nadzor nad izvajanjem odločbe vlade iz prvega odstavka 117. člena tega zakona.«;

8. se v 289. členu črta tretji odstavek;

9. se v 298. členu v prvem odstavku:

– doda nova 1. točka, ki se glasi:

»1. ne izvede odločbe vlade iz prvega odstavka 117. člena tega zakona,«;

– dosedanje 1. do 10. točka postanejo 2. do 11. točka;

10. se v 299. členu v prvem odstavku:

– 22., 23. in 24. točka spremenijo tako, da se glasijo:

»22. ne določi SUVI ali SUNP kot poslovno skrivnost v skladu z drugim odstavkom 115. člena tega zakona,

23. ne sprejme, pregleduje ali posodobi SUNP v delu, ki se nanaša na komunikacije v sili, s predhodno odobritvijo pristojnih organov, ki so odgovorni za delovanje centrov za sprejem komunikacije v sili, v skladu s tretjim odstavkom 115. člena tega zakona,

24. ne upošteva splošnega akta agencije iz četrtega odstavka 115. člena tega zakona,«;

– 26., 27., 28. in 29. točka črtajo;

– dosedanje 30. do 119. točka postanejo 26. do 115. točka.

66. člen

(dopolnitev Zakona o dostopu do informacij javnega značaja)

V Zakonu o dostopu do informacij javnega značaja (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US, 102/15, 7/18 in 141/22) se v 6. členu v prvem odstavku na koncu 11. točke pika nadomesti s podpičjem in doda nova 12. točka, ki se glasi:

»12. podatek, ki je opredeljen kot varovani podatek pristojnega nacionalnega organa v skladu z zakonom, ki ureja informacijsko varnost.«.

67. člen

(sprememba Zakona o varstvu osebnih podatkov)

V Zakonu o varstvu osebnih podatkov (Uradni list RS, št. 163/22) se v 23. členu v prvem odstavku besedilo »o varnostnih zahtevah« nadomesti z besedilom »o ukrepih za obvladovanje tveganj«, besedilo »izvajalce bistvenih storitev« pa se nadomesti z besedilom » bistvene subjekte«.

68. člen

(dokončanje postopkov, začetih pred uveljavitvijo tega zakona)

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

XII. KONČNI DOLOČBI

69. 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:

– 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) Z dnem uveljavitve tega zakona prenehata veljati:

– Splošni akt o obveščanju in vrednotenju varnostnih incidentov ter o najavi omejitev ali prekinitev (Uradni list RS, št. 74/23), ki se še naprej uporablja v delu, ki se nanaša na najavo omejitev ali prekinitev, in

– Splošni akt o varnosti omrežij, storitev in podatkov (Uradni list, št. 106/23).

70. člen

(začetek veljavnosti)

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

Št. 011-02/25-7/21

Ljubljana, dne 23. maja 2025

EPA 2057-IX

Državni zbor

Republike Slovenije
mag. Urška Klakočar Zupančič
predsednica

Priloga 1: Visoko kritični sektorji

Priloga 2: Drugi kritični sektorji

Priloga 3: Drugi subjekti javne uprave na državni ravni