Z A K O N
O INFORMACIJSKI VARNOSTI (ZInfV)

I. Splošne določbe

1. člen
(vsebina zakona)

Ta zakon ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji. Določa minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona. Prav tako ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: pristojni nacionalni organ), enotne kontaktne točke za informacijsko varnost (v nadaljnjem besedilu: enotna kontaktna točka), nacionalne skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljnjem besedilu: nacionalni CSIRT) in skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (v nadaljnjem besedilu: CSIRT organov državne uprave) na področju zagotavljanja informacijske varnosti.

2. člen
(namen in področje uporabe zakona)

(1) Namen zakona je ureditev področja informacijske varnosti in zagotovitev visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah in zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti.

(2) S tem zakonom se v pravni red Republike Slovenije prenaša Direktiva (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L št. 194 z dne 19. 7. 2016, str. 1), (v nadaljnjem besedilu: Direktiva 2016/1148/ES).

(3) Ta zakon se ne uporablja za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve (operaterji), za katere veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev iz zakona, ki ureja elektronske komunikacije, ter za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (UL L št. 257 z dne 28. 8. 2014, str. 73).

3. člen
(obdelava podatkov)

(1) Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov.

(2) Podatki in informacije, ki se obdelujejo na podlagi tega zakona in so opredeljeni kot tajni ali kot poslovna skrivnost, se obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost.

4. člen
(pomen izrazov)

Izrazi, uporabljeni v tem zakonu, imajo za potrebe tega zakona naslednji pomen:

1. Bistvena storitev je storitev, ki se zagotavlja na področjih iz drugega odstavka 5. člena tega zakona, in je bistvena za ohranitev ključnih družbenih in gospodarskih dejavnosti.
2. CSIRT je skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov.
3. Digitalna infrastruktura so stičišča omrežij, register domenskih imen najvišje ravni in ponudniki storitev sistema domenskih imen.
4. Digitalna storitev so naslednje storitve informacijske družbe: storitve spletne tržnice, spletnega iskalnika in računalništva v oblaku.
5. Incident je vsak dogodek, ki ima dejanski negativen učinek na varnost omrežij in informacijskih sistemov.
6. Informacijsko okolje je skupek družbenih omrežij in kibernetskega prostora, vključno z informacijami.
7. Informacijska varnost je zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti.
8. Izvajalec bistvenih storitev je javni ali zasebni subjekt, ki spada v katero od področij, navedenih v 5. členu tega zakona, in izpolnjuje merila, določena v 7. členu tega zakona, ter dodatna področna merila, določena s predpisi.
9. Kibernetska grožnja je možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov.
10. Kibernetska obramba je celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju.
11. Kibernetska varnost je sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi.
12. Kibernetski napad je napad prek kibernetskega prostora z namenom zlonamernega uničevanja, izpostavljanja, nadzorovanja ali spreminjanja, onemogočanja, zbiranja in oviranja kateregakoli dela kibernetskega prostora, vključno glede informacij, ki so bistvenega pomena za nemoteno delovanje države.
13. Kibernetski prostor je globalno informacijsko okolje, ustvarjeno s pomočjo elektronsko komunikacijskih omrežij in informacijskih sistemov. Kibernetski prostor omogoča nastanek, obdelavo in izmenjavo informacij.
14. Ključni deli nacionalnega varnostnega sistema so omrežja in informacijski sistemi, namenjeni področju obrambe, varstva pred naravnimi in drugimi nesrečami, policije, obveščevalno-varnostne dejavnosti ter zunanjih zadev.
15. Ključni informacijski sistemi so vsi informacijski sistemi subjekta, brez katerih ni mogoče neprekinjeno izvajati storitev.
16. Krmilni informacijski sistemi so informacijski sistemi, ki omogočajo izvajanje pravilnih postopkov in izvajajo ustrezno sosledje delovanja ključnih informacijskih sistemov subjekta.
17. Kvalificiran revizor je revizor s področja informacijske varnosti, ki je certifikat pridobil pri eni izmed neodvisnih revizijskih organizacij.

18. Mreža skupin CSIRT je povezava, v kateri sodelujejo skupine CSIRT iz držav članic in CERT-EU.
19. Nacionalni center za krizno upravljanje je center, določen v predpisu, ki ureja organizacijo in delovanje nacionalnega centra za krizno upravljanje.
20. Nadzorni informacijski sistemi so informacijski sistemi, ki skrbijo za izvajanje nadzorstvene funkcije informacijskih sistemov subjekta.
21. Obvladovanje incidentov so vsi postopki, ki omogočajo odkrivanje, analizo in zajezitev incidentov ter odzivanje nanje.
22. Omrežje in informacijski sistem so:
    - elektronsko komunikacijsko omrežje, ki vključuje prenosne sisteme in, kjer je primerno, komutacijsko ali usmerjevalno opremo ter druge vire, vključno z omrežnimi elementi, ki niso aktivni, ki omogočajo prenos signalov po žicah, z radijskimi valovi, z optičnimi ali drugimi elektromagnetnimi sredstvi, vključno s satelitskimi omrežji, fiksnimi (vodovno in paketno komutiranimi, vključno z internetom) in mobilnimi prizemnimi omrežji, električnimi kabelskimi sistemi, če se uporabljajo za prenos signalov, omrežij, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kabelske televizije, ne glede na vrsto prenesenih informacij;
    - vsaka naprava ali skupina med seboj povezanih ali sorodnih naprav, od katerih ena ali več njih na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali
    - digitalni podatki, ki jih elementi iz prve in prejšnje alineje te točke shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja.
23. Ponudnik digitalnih storitev je vsaka fizična ali pravna oseba, ki zagotavlja digitalno storitev.
24. Ponudnik storitev sistema domenskih imen je subjekt, ki zagotavlja storitve sistema domenskih imen na internetu.
25. Predstavnik je vsaka fizična ali pravna oseba s sedežem v Evropski uniji (v nadaljnjem besedilu: EU), ki je izrecno določena, da deluje v imenu ponudnika digitalnih storitev, ki nima sedeža v Uniji, in s katero lahko pristojni nacionalni organ ali nacionalni CSIRT vzpostavi stik namesto s ponudnikom digitalnih storitev, kar zadeva obveznosti tega ponudnika digitalnih storitev na podlagi tega zakona.
26. Register domenskih imen najvišje ravni je subjekt, ki upravlja in izvaja registracijo imen internetnih domen v okviru določene domene najvišje ravni.
27. Revizijska sled je nespremenljiva sled oziroma niz podatkov, ki se je zgodil v informacijskem sistemu ali napravi, z natančnim časovnim zapisom v obliki dnevniškega zapisa, ki omogoča natančen pregled vseh zapisov, povezanih z vsemi dogodki in vsemi shranjenimi informacijami, od nastanka podatka ali informacije naprej do trenutnega stanja.
28. Sistem domenskih imen je hierarhičen porazdeljen sistem dodeljevanja imen v omrežju, ki posreduje poizvedbe za domenska imena.
29. Skupina za sodelovanje je skupina, ki jo sestavljajo predstavniki držav članic EU, Evropske komisije in Agencije Evropske unije za varnost omrežij in informacij (agencija ENISA).
30. Specifikacija je dokument, ki predpisuje tehnične zahteve, ki jih mora izpolniti proizvod, proces, storitev ali sistem.
31. Spletna tržnica je digitalna storitev, ki potrošnikom (vsaka fizična oseba, ki deluje za namene zunaj okvira svoje trgovske, poslovne, obrtne ali poklicne dejavnosti) oziroma trgovcem (vsaka fizična ali pravna oseba v zasebni ali javni lasti, ki sama ali prek osebe, ki nastopa v njenem imenu ali po njenem naročilu, deluje za namene v zvezi s svojo trgovsko, poslovno, obrtno ali poklicno dejavnostjo) omogoča, da na spletišču spletne tržnice ali na spletišču trgovca, ki uporablja računalniške storitve spletne tržnice, s trgovci sklenejo pogodbe o spletni prodaji ali pogodbe o spletnih storitvah.
32. Spletni iskalnik je digitalna storitev, ki uporabnikom na podlagi poizvedbe o katerikoli temi v obliki ključne besede, fraze ali drugega vnosa omogoča iskanje po načeloma vseh

spletiščih ali spletiščih v določenem jeziku, ponudi pa povezave do strani z informacijami o zahtevani vsebini.

33. Standard je tehnična specifikacija, ki jo je sprejel priznan organ za standardizacijo za večkratno ali stalno uporabo.
34. Stičišče omrežij je omrežna zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih avtonomnih sistemov, predvsem zaradi izmenjave internetnega prometa in zagotavlja medsebojno povezavo le avtonomnih sistemov ter omogoča izmenjavo internetnega prometa med katerimakoli sodelujočima avtonomnima sistemoma, brez prehoda prek tretjega avtonomnega sistema, prav tako pa ne spreminja takšnega prometa ali kako drugače posega vanj.
35. Storitev informacijske družbe je katerakoli storitev, ki se običajno opravi odplačno, na daljavo (storitev se opravi, ne da bi bile stranke sočasno navzoče), elektronsko (storitev se pošlje na začetnem kraju in sprejme na cilju z elektronsko opremo za obdelavo in shranjevanje podatkov ter se v celoti prenaša, pošilja in sprejema po žici, radijsko, z optičnimi ali drugimi elektromagnetnimi sredstvi) in na posamezno zahtevo prejemnika storitev (storitev opravi s prenosom podatkov na posamezno zahtevo).
36. Storitev računalništva v oblaku je digitalna storitev, ki omogoča dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov.
37. Strategija kibernetske varnosti je nacionalna strategija za varnost omrežij in informacijskih sistemov ter pomeni okvir s strateškimi cilji in prednostnimi nalogami na področju varnosti omrežij in informacijskih sistemov v Republiki Sloveniji.
38. Tveganje je vsaka razumno določljiva okoliščina ali dogodek, ki ima lahko negativen učinek na varnost omrežij in informacijskih sistemov.
39. Varnost omrežij in informacijskih sistemov je zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vse dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali pripadajočih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopni.
40. Varnostno operativni center je notranja organizacijska enota posameznih organov državne uprave, ki se odziva na incidente na področju informacijske varnosti.

II. Zavezanci

5. člen
(zavezanci)

(1) Zavezanci po tem zakonu so:

- izvajalci bistvenih storitev,
- ponudniki digitalnih storitev in
- organi državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljnjem besedilu: organi državne uprave).

(2) Izvajalci bistvenih storitev so subjekti, ki delujejo na naslednjih področjih:

1. energija,
2. digitalna infrastruktura,
3. oskrba s pitno vodo in njena distribucija,
4. zdravstvo,
5. promet,
6. bančništvo,
7. infrastruktura finančnega trga,
8. preskrba s hrano in
9. varstvo okolja.

6. člen
(določitev izvajalcev bistvenih storitev)

(1) Za namen določitve izvajalcev bistvenih storitev Vlada Republike Slovenije (v nadaljnjem besedilu: vlada) določi seznam bistvenih storitev iz predpisa, ki ureja standardno klasifikacijo dejavnosti.

(2) Posameznega izvajalca bistvenih storitev na podlagi meril iz 7. člena tega zakona določi vlada.

(3) Ne glede na določbo prejšnjega odstavka vlada kot izvajalce bistvenih storitev določi tudi tiste upravljavce kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo področje kritične infrastrukture, in nosilce obrambnega načrtovanja, ki so določeni v skladu s predpisi, ki urejajo področje obrambe, katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov.

(4) Če izvajalec zagotavlja bistveno storitev v Republiki Sloveniji in še kateri drugi državi članici EU, se pristojni nacionalni organ pred določitvijo izvajalcev bistvenih storitev iz drugega odstavka ali prejšnjega odstavka tega člena v skladu z Direktivo 2016/1148/ES posvetuje s pristojnim nacionalnim organom države članice EU, kjer izvajalec takšne storitve zagotavlja.

7. člen
(merila − metodologija)

(1) Pri določitvi izvajalcev bistvenih storitev iz drugega odstavka 5. člena tega zakona se upošteva naslednja merila:
- subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih oziroma gospodarskih dejavnosti;
- zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov in
- incident bi imel pomemben negativen vpliv na zagotavljanje te storitve.

(2) Pri določanju, kako pomemben je negativen vpliv iz tretje alineje prejšnjega odstavka, se upoštevajo vsaj trije od naslednjih medpodročnih dejavnikov:
1. število uporabnikov, ki so odvisni od storitve subjekta;
2. odvisnost drugih področij iz drugega odstavka 5. člena tega zakona od storitve subjekta;
3. stopnja in trajanje vpliva, ki bi ga incidenti lahko imeli na gospodarske in družbene dejavnosti ali javno varnost;
4. tržni delež subjekta;
5. geografska razširjenost, kar zadeva območje, ki bi ga incident lahko prizadel;
6. pomen subjekta za ohranitev zadostne ravni storitve, ob upoštevanju razpoložljivosti alternativnih načinov za zagotavljanje storitve.

(3) Pri odločanju, ali bi incident imel pomemben negativen vpliv, se upoštevata vsaj dva od naslednjih področnih dejavnikov:
- število uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvene storitve;
- trajanje incidenta;
- geografska razširjenost, kar zadeva območje, na katerega vpliva incident.

(4) Metodologijo za določitev izvajalcev bistvenih storitev podrobneje določi vlada.

8. člen
(določitev ponudnikov digitalnih storitev)

(1) Ponudniki digitalnih storitev iz druge alineje prvega odstavka 5. člena tega zakona so zavezanci za izpolnjevanje obveznosti po tem zakonu.

(2) Ne glede na prejšnji odstavek niso zavezanci ponudniki digitalnih storitev, ki imajo manj kot 50 zaposlenih in imajo letni promet oziroma letno bilančno vsoto, ki ne presega deset milijonov eurov.

9. člen
(določitev organov državne uprave)

(1) Vlada določi organe državne uprave iz tretje alineje prvega odstavka 5. člena tega zakona in CSIRT organov državne uprave.

(2) Ne glede na prejšnji odstavek se CSIRT organov državne uprave ne določi, če imajo organi državne uprave v svoji notranji organizacijski strukturi zagotovljene lastne zmogljivosti vsaj na ravni varnostno operativnega centra.

10. člen
(določitev kontaktne osebe zavezancev)

(1) Izvajalec bistvene storitve v 15 dneh od odločitve iz drugega odstavka 6. člena tega zakona določi kontaktno osebo za informacijsko varnost in njenega namestnika ter pristojnemu nacionalnemu organu posreduje njune kontaktne podatke.

(2) Organ državne uprave lahko določi kontaktno osebo za informacijsko varnost in njenega namestnika ter pristojnemu nacionalnemu organu posreduje njune kontaktne podatke.

(3) Ponudnik digitalnih storitev, ki ima skladno s prvim odstavkom 15. člena tega zakona glavni sedež v Republiki Sloveniji, lahko določi in pooblasti kontaktno osebo za informacijsko varnost in njenega namestnika ter te kontaktne podatke posredujejo pristojnemu nacionalnemu organu.

(4) Če ponudnik digitalnih storitev nima sedeža v EU, vendar določi sedež svojega predstavnika za EU v Republiki Sloveniji skladno z drugim odstavkom 15. člena tega zakona, ta predstavnik velja za njegovo kontaktno osebo. Kontaktne podatke predstavnika lahko ponudniki digitalnih storitev posredujejo pristojnemu nacionalnemu organu.

(5) Zavezanci iz prvega odstavka tega člena o spremembi kontaktnih podatkov obvestijo pristojni nacionalni organ v roku 15 delovnih dni po nastali spremembi.

III. Informacijska varnost izvajalcev bistvenih storitev

11. člen
(varnostne zahteve)

(1) Izvajalci bistvenih storitev skladno z metodologijo iz tretjega odstavka 12. člena tega zakona, določijo svoje ključne, krmilne in nadzorne informacijske sisteme ter dele omrežja, s katerimi zagotavljajo izvajanje bistvenih storitev.

(2) Izvajalci bistvenih storitev izvedejo analizo, oceno in vrednotenje tveganj ter na tej osnovi pripravijo in izvedejo potrebne ukrepe za obvladovanje tveganj glede varnosti omrežij in informacijskih sistemov, ki jih uporabljajo pri bistvenih storitvah.

(3) Izvajalci bistvenih storitev sprejmejo ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost tistih omrežij in informacijskih sistemov, ki se uporabljajo za zagotavljanje bistvenih storitev, da bi zagotovili neprekinjeno izvajanje teh storitev.

(4) Če izvajalci bistvenih storitev za opravljanje svoje dejavnosti črpajo vhodne podatke in informacije iz ključnih delov nacionalno varnostnega sistema, vzpostavijo vse potrebne varnostne zahteve ob soglasju pristojnega ministrstva za posamezni ključni del nacionalno varnostnega sistema.

12. člen
(varnostna dokumentacija in varnostni ukrepi)

(1) Izvajalci bistvenih storitev za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj:

1. analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj;
2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja;
3. seznam njegovih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev;
4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje;
5. načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT;
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo področne posebnosti.

(2) Izvajalci bistvenih storitev na podlagi varnostne dokumentacije iz prejšnjega odstavka pripravijo in izvajajo potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe.

(3) Minister, pristojen za informacijsko družbo (v nadaljnjem besedilu: minister) podrobneje določi vsebino in strukturo varnostne dokumentacije iz prvega odstavka tega člena ter minimalen obseg in vsebino varnostnih ukrepov iz prejšnjega odstavka. Pri tem predpiše tudi metodologiji za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov iz 2. in 3. točke prvega odstavka tega člena.

(4) Če ima izvajalec bistvenih storitev za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo dopolni skladno s tem zakonom.

(5) Izvajalci bistvenih storitev za namen obvladovanja incidentov, skladno z analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj in ob upoštevanju stanja tehnike zagotovijo tudi ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja, za obdobje šestih mesecev. Ohranjanje dnevniških zapisov se zagotavlja na ozemlju Republike Slovenije, razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, glede katerih se lahko zagotavlja na ozemlju EU.

13. člen
(priglasitev incidentov)

(1) Izvajalci bistvenih storitev nacionalnemu CSIRT brez nepotrebnega odlašanja priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev, ki jih zagotavljajo.

Priglasitev zajema informacije, na podlagi katerih je mogoče določiti morebiten čezmejni vpliv incidenta. Izvajalci bistvenih storitev pri določitvi pomembnosti vpliva incidenta upoštevajo zlasti:
- število uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvene storitve,
- trajanje incidenta in
- geografska razširjenost, kar zadeva območje, na katerega incident vpliva.

(2) Priglasitelj mora ob prijavi incidenta poskrbeti za ustrezno zavarovanje dnevniških zapisov oziroma revizijskih sledi, če te obstajajo.

(3) Nacionalni CSIRT o incidentu obvesti pristojni nacionalni organ, ki vodi seznam incidentov iz tretjega odstavka 25. člena tega zakona. Pristojni nacionalni organ o incidentu, ki bi lahko imel večji medpodročni vpliv oziroma bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti Republike Slovenije, nemudoma obvesti policijo ter Nacionalni center za krizno upravljanje.

(4) Če ima incident pomemben vpliv na neprekinjenost izvajanja bistvenih storitev v drugi državi članici EU, pristojni nacionalni organ ali nacionalni CSIRT o tem obvesti enotno kontaktno točko v prizadeti državi oziroma državah članicah EU. Pri tem zaščiti varnost in poslovne interese izvajalca bistvenih storitev ter zaupnost informacij, ki jih slednji zagotovi v svoji priglasitvi.

(5) Informacije in podatki iz prejšnjega odstavka, ki so zaupni, se posredujejo, če je to potrebno za uporabo Direktive 2016/1148/ES oziroma za izvajanje tega zakona. Posredovanje je omejeno na obseg, ki je primeren in nujen glede na namen iz prejšnjega odstavka ter mora ohraniti zaupnost posredovanih informacij in podatkov.

(6) Pri izvajanju obveznosti priglasitve mora nacionalni CSIRT paziti, da informacije o ranljivosti bistvene storitve ostanejo zaupne, dokler se varnost znova ne vzpostavi.

(7) Če nacionalni CSIRT presodi, da je to potrebno, izvajalcu bistvenih storitev po priglasitvi incidenta posreduje ustrezne informacije glede nadaljnjih ukrepov na podlagi njegove priglasitve, ki bi lahko prispevale k učinkovitemu obvladovanju incidenta.

(8) Pristojni nacionalni organ lahko po posvetovanju z izvajalcem bistvenih storitev, ki je priglasil incident, obvesti javnost o posameznih incidentih, kadar je ozaveščenost javnosti potrebna za njegovo obravnavo ali zaradi preprečitve stopnjevanja incidenta ali novih incidentov.

(9) Pri obveščanju javnosti iz prejšnjega odstavka pristojni nacionalni organ upošteva ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani, ter morebitno škodo za ugled in poslovanje izvajalcev bistvenih storitev, ki priglasijo incidente, na drugi strani.

IV. Informacijska varnost ponudnikov digitalnih storitev

14. člen
(varnostne zahteve in priglasitev incidentov)

(1) Ponudniki digitalnih storitev določijo in sprejmejo primerne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju teh storitev v EU. Ob upoštevanju stanja tehnike s temi ukrepi zagotovijo raven varnosti omrežij in informacijskih sistemov, ki je primerna obstoječemu tveganju. Pri tem upoštevajo naslednje elemente:
- varnost sistemov in zmogljivosti,
- obvladovanje incidentov,
- upravljanje neprekinjenega poslovanja,
- spremljanje, revidiranje in preizkušanje ter
- skladnost z mednarodnimi standardi.

(2) Ponudniki digitalnih storitev sprejmejo ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov, na ponujane storitve, ki jih zagotavljajo v EU, da bi zagotovili neprekinjeno izvajanje teh storitev.

(3) Ponudniki digitalnih storitev vsak incident, ki ima pomemben vpliv na zagotavljanje teh storitev, ki jih ponujajo v EU, brez nepotrebnega odlašanja priglasijo nacionalnemu CSIRT. Priglasitev zajema informacije, na podlagi katerih lahko nacionalni CSIRT določi pomembnost morebitnega čezmejnega vpliva. Obveznost priglasitve incidenta velja le, kadar ima ponudnik digitalnih storitev dostop do informacij, potrebnih za oceno vpliva incidenta glede na parametre iz petega odstavka tega člena.

(4) Nacionalni CSIRT o incidentu obvesti pristojni nacionalni organ, ki vodi seznam incidentov iz tretjega odstavka 25. člena tega zakona. Pristojni nacionalni organ o incidentu, ki bi lahko imel večji medpodročni vpliv oziroma bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti Republike Slovenije, nemudoma obvesti policijo ter Nacionalni center za krizno upravljanje.

(5) Pri določitvi stopnje vpliva incidenta se upoštevajo zlasti naslednji parametri:
- število uporabnikov, na katere vpliva incident, zlasti uporabnikov, ki so odvisni od storitve pri zagotavljanju lastnih storitev,
- trajanje incidenta,
- geografska razširjenost, kar zadeva območje, na katerega incident vpliva,
- v kakšnem obsegu je moteno delovanje storitve in
- obseg vpliva na gospodarske in družbene dejavnosti.

(6) Kadar je izvajalec bistvenih storitev pri zagotavljanju storitve, ki je bistvena za ohranitev ključnih družbenih in gospodarskih dejavnosti, odvisen od tretjega ponudnika digitalnih storitev, ta izvajalec bistvenih storitev priglasi vsak znaten vpliv na neprekinjeno izvajanje bistvenih storitev, ki je posledica incidenta, ki vpliva na ponudnika digitalnih storitev.

(7) Pristojni nacionalni organ obvesti druge prizadete države članice EU, če incident zadeva dve ali več držav članic EU ali v drugih primerih, če oceni, da bi obvestilo drugih držav članic EU prispevalo k izboljšanju ravni varnosti omrežij in informacijskih sistemov.

(8) Posredovanje informacij in podatkov iz prejšnjega odstavka, ki so zaupni, je omejeno na obseg, ki je ustrezen in sorazmeren glede na namen te izmenjave.

(9) Pri izvajanju obveznosti priglasitve mora nacionalni CSIRT paziti, da informacije o ranljivosti digitalne storitve ostanejo zaupne, dokler se varnost znova ne vzpostavi.

(10) Pristojni nacionalni organ lahko po posvetovanju z zadevnim ponudnikom digitalnih storitev obvesti javnost o posameznih incidentih ali zahteva, da to stori ponudnik digitalnih storitev, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki že poteka, ali kadar je razkritje incidenta kako drugače v javnem interesu.

(11) Kadar javnost na podlagi prejšnjega odstavka obvešča pristojni nacionalni organ upošteva ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani, ter morebitno škodo za ugled in poslovanje ponudnikov digitalnih storitev, ki priglasijo incidente, na drugi strani.

15. člen
(pristojnost in teritorialnost)

(1) Ponudnik digitalnih storitev, ki ima glavni sedež v Republiki Sloveniji, spada v pristojnost pristojnega nacionalnega organa in nacionalnega CSIRT, ki mu priglaša incidente. Za namene tega zakona se šteje, da ima prej navedeni ponudnik digitalnih storitev glavni sedež v Republiki Sloveniji, če ima v Republiki Sloveniji glavno upravo.

(2) Če ponudnik digitalnih storitev, ki nima sedeža v EU, v njej pa zagotavlja takšne storitve, določi sedež svojega predstavnika za EU v Republiki Sloveniji, kjer tudi zagotavlja digitalne storitve, spada v pristojnost pristojnega nacionalnega organa in nacionalnega CSIRT. Predstavnik zastopa ponudnika digitalnih storitev v zvezi z obveznostmi na podlagi tega zakona.

(3) Če ima ponudnik digitalnih storitev glavni sedež ali predstavnika v eni državi članici EU, omrežja in informacijske sisteme pa v drugi ali več drugih državah članicah EU, pristojni nacionalni organ v primeru, da je delovanje tega ponudnika digitalnih storitev kakorkoli povezano z Republiko Slovenijo, sodeluje glede na okoliščine primera s pristojnim organom iz države članice EU, kjer je glavni sedež ponudnika digitalnih storitev ali njegovega predstavnika v EU, oziroma z zadevnimi pristojnimi organi teh drugih držav članic EU. Takšno sodelovanje lahko zajema izmenjavo informacij med pristojnimi organi in zahteve za sprejem ustreznih nadzornih ukrepov iz poglavja o inšpekcijskem nadzoru tega zakona.

(4) Informacije in podatki iz prejšnjega odstavka, ki so zaupni, se posredujejo, če je to potrebno za uporabo Direktive 2016/1148/ES oziroma za izvajanje tega zakona. Posredovanje je omejeno na obseg, ki je primeren in nujen glede na namen iz prejšnjega odstavka ter mora ohraniti zaupnost posredovanih informacij in podatkov.

V. Informacijska varnost organov državne uprave

16. člen
(varnostne zahteve)

(1) Organi državne uprave morajo izvesti analizo, oceno in vrednotenje tveganj ter na tej podlagi pripraviti in izvesti ukrepe, potrebne za obvladovanje tveganj glede varnosti za informacijske sisteme in dele omrežja, s katerimi upravljajo (v nadaljnjem besedilu: omrežja in informacijski sistemi organov državne uprave), oziroma za informacijske storitve, ki jih

izvajajo in so nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljnjem besedilu: storitve organov državne uprave).

(2) Organi državne uprave sprejmejo potrebne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost omrežij in informacijskih sistemov državnih organov, da bi zagotovili neprekinjeno izvajanje storitev organov državne uprave.

(3) Če organi državne uprave za opravljanje svoje dejavnosti črpajo vhodne podatke in informacije iz ključnih delov nacionalno varnostnega sistema, vzpostavijo vse potrebne varnostne zahteve ob soglasju pristojnega ministrstva za posamezni ključni del nacionalno varnostnega sistema.

17. člen
(varnostna dokumentacija in varnostni ukrepi)

(1) Organi državne uprave za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov državnih organov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj:

1. analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj,
2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja,
3. seznam informacijskih sistemov in delov omrežja organov državne uprave ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev organov državne uprave,
4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje,
5. načrt odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave in
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov organov državne uprave.

(2) Organi državne uprave na podlagi varnostne dokumentacije iz prejšnjega odstavka pripravijo in izvajajo potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe.

(3) Minister podrobneje določi vsebino in strukturo varnostne dokumentacije iz prvega odstavka tega člena ter minimalen obseg in vsebino varnostnih ukrepov iz prejšnjega odstavka. Pri tem predpiše tudi metodologiji za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov iz 2. in 3. točke prvega odstavka tega člena.

(4) Če ima organ državne uprave za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo dopolni skladno s tem zakonom.

(5) Organi državne uprave za namen obvladovanja incidentov, skladno z analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj, ki jo izvedejo ob upoštevanju stanja tehnike, zagotovijo tudi ohranjanje dnevniških zapisov o delovanju svojih informacijskih sistemov ali delov omrežja za obdobje šestih mesecev. Ohranjanje teh dnevniških zapisov mora biti zagotovljeno na ozemlju Republike Slovenije.

18. člen
(priglasitev incidentov)

(1) Organi državne uprave brez nepotrebnega odlašanja CSIRT organov državne uprave priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje storitev organov državne uprave, tisti organi državne uprave, ki imajo lastne zmogljivosti vsaj na ravni varnostno operativnega centra, pa pristojnemu nacionalnemu organu. Pri določitvi pomembnosti vpliva incidenta upoštevajo zlasti:

- število uporabnikov, ki jih je prizadela motnja pri zagotavljanju storitve organov državne uprave,
- trajanje incidenta in
- geografsko razširjenost, kar zadeva območje, na katerega vpliva incident.

(2) Priglasitelj mora ob prijavi incidenta poskrbeti za ustrezno zavarovanje dnevniških zapisov oziroma revizijskih sledi, če te obstajajo.

(3) CSIRT organov državne uprave o incidentu obvesti nacionalni CSIRT in pristojni nacionalni organ, ki vodi seznam incidentov iz tretjega odstavka 25. člena tega zakona. Pristojni nacionalni organ o incidentu, ki bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti Republike Slovenije, nemudoma obvesti policijo ter Nacionalni center za krizno upravljanje.

(4) Pri izvajanju obveznosti priglasitve mora CSIRT organov državne uprave paziti, da informacije o ranljivosti storitve organa državne uprave ostanejo zaupne, dokler se varnost znova ne vzpostavi.

(5) Pristojni nacionalni organ lahko po posvetovanju z organom državne uprave, ki je priglasil incident, obvesti javnost o posameznih incidentih, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali njegovo obravnavo.

(6) Pri obveščanju javnosti iz prejšnjega odstavka pristojni nacionalni organ upošteva ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani ter morebitnim negativnim vplivom takšne objave na preiskovanje ali pregon kaznivih dejanj, javni red in mir, nacionalno varnost in obrambo države na drugi strani.

VI. Standardizacija in prostovoljna priglasitev

19. člen
(standardizacija)

Za uskladitev pristopov izvajalcev bistvenih storitev, ponudnikov digitalnih storitev in organov državne uprave pri izvajanju obveznosti iz tretjega, četrtega in petega poglavja tega zakona pristojni nacionalni organ z namenom spodbujanja uporabe evropskih ali mednarodno sprejetih standardov in specifikacij, pomembnih za varnost omrežij in informacijskih sistemov, te informacije objavlja na svoji spletni strani.

20. člen
(prostovoljna priglasitev)

(1) Subjekti, ki niso bili določeni kot zavezanci po tem zakonu, lahko prostovoljno priglasijo incidente, ki imajo pomemben vpliv na neprekinjeno izvajanje storitev, ki jih zagotavljajo. Pri tem subjekti javnega sektorja, ki niso organi državne uprave iz 9. člena tega zakona, ravnajo v skladu s postopkom iz 18. člena tega zakona, subjekti zasebnega sektorja pa skladno s postopkom iz 13. člena tega zakona.

(2) Nacionalni CSIRT in CSIRT organov državne uprave pred prostovoljnimi priglasitvami prednostno obdelata obvezne priglasitve. Pri določanju vrstnega reda obdelave prostovoljnih priglasitev upoštevata vpliv prostovoljno priglašenih incidentov na neprekinjeno izvajanje bistvenih storitev, storitev organov državne uprave ter čezmejni vpliv incidenta.

(3) Prostovoljno priglašene incidente, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje bistvenih storitev, storitev organov državne uprave in imajo zanemarljiv čezmejni vpliv, se obdela le, kadar takšna obdelava nacionalnemu CSIRT ali CSIRT organov državne uprave ne pomeni nesorazmernega ali neupravičenega bremena.

VII. Vrednotenje incidenta, stanje povečane ogroženosti in kibernetska obramba

21. člen
(vrednotenje incidenta in ukrepanje)

(1) Priglašene incidente ob njihovem reševanju vrednoti pristojni nacionalni CSIRT ali CSIRT organov državne uprave, v primeru, da imajo organi državne uprave zagotovljene lastne zmogljivosti vsaj na ravni varnostno operativnega centra, pa jih vrednoti pristojni nacionalni organ. Pri vrednotenju se lahko navedeni organi medsebojno posvetujejo. Pri tem je glede na težo incidenta:

- lažji incident enkraten incident, ki ima glede na parametre določitve pomembnosti vpliva incidenta iz prvega odstavka 13. člena ali petega odstavka 14. člena ali prvega odstavka 18. člena tega zakona majhen negativen vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev zavezanca in ne sme imeti večjega vpliva na nemoteno delovanje zavezanca ter mu povzročiti večje škode. Prav tako takšen incident ne sme imeti negativnega medpodročnega vpliva ali negativnega vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja;
- težji incident enkraten incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju, ki ima glede na parametre določitve pomembnosti vpliva incidenta iz prvega odstavka 13. člena ali petega odstavka 14. člena ali prvega odstavka 18. člena tega zakona velik negativen vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev zavezanca. Takšen incident ima pomemben vpliv na nemoteno delovanje zavezanca in mu povzroči večjo škodo. Ob tem ima takšen incident lahko tudi negativen medpodročni vpliv oziroma negativen vpliv na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja, vendar ta vpliv ne dosega kriterijev iz naslednje alineje;
- kritični incident tisti incident, ki ima glede na parametre določitve pomembnosti vpliva incidenta iz prvega odstavka 13. člena ali petega odstavka 14. člena ali prvega odstavka 18. člena tega zakona zelo velik negativen vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev zavezanca. Ob tem takšen incident povzroči tudi oteženo delovanje države, še posebej informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja, oziroma delno onemogoči delovanje vsaj treh področij bistvenih storitev ali enega v celoti.

(2) Pristojni nacionalni organ na podlagi podatkov in informacij o teži incidenta iz prejšnjega odstavka, ki mu jih sproti posredujeta nacionalni CSIRT ali CSIRT organov državne uprave, oceni ali gre hkrati tudi za kibernetski napad.

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

(4) Pristojni nacionalni organ lahko zavezancu v primeru težjega ali kritičnega incidenta ali v primeru kibernetskega napada s pisno odločbo, v nujnih primerih pa tudi ustno, določi takšne primerne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic. Zavezancu se pisni odpravek ustne odločbe vroči čim prej, vendar najkasneje v roku 48 ur po ustni odločbi.

(5) Ukrepi, izdani na podlagi prejšnjega odstavka, se določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz prejšnjega odstavka. Pritožba zoper odločbo iz prejšnjega odstavka ne zadrži njene izvršitve.

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

22. člen
(stanje povečane ogroženosti in ukrepanje)

(1) Stanje povečane ogroženosti varnosti omrežij ali informacijskih sistemov (v nadaljnjem besedilu: stanje povečane ogroženosti) je stanje, ko je podana velika verjetnost realizacije težjega ali kritičnega incidenta iz prvega odstavka oziroma kibernetskega napada iz drugega odstavka prejšnjega člena v 72 urah od zaznave takšne verjetnosti.

(2) Pristojni nacionalni organ glede na podatke in informacije, s katerimi razpolaga, in v sodelovanju s preostalimi pristojnimi organi oceni, ali gre za stanje povečane ogroženosti iz prejšnjega odstavka.

(3) Pristojni nacionalni organ mora o stanju povečane ogroženosti zaradi verjetnosti realizacije kritičnega incidenta ali kibernetskega napada iz prvega odstavka tega člena nemudoma obvestiti vlado in SNAV, lahko pa ju glede na presojo relevantnih okoliščin obvesti tudi zaradi verjetnosti realizacije težjega incidenta iz prvega odstavka tega člena.

(4) Pristojni nacionalni organ lahko v stanju povečane ogroženosti zavezancu iz prve ali tretje alineje prvega odstavka 5. člena tega zakona s pisno odločbo, v nujnih primerih pa tudi ustno, določi takšne primerne in sorazmerne ukrepe, kot je potrebno za preprečitev ali za zmanjšanje verjetnosti realizacije incidenta iz prvega odstavka tega člena, kot tudi za zmanjšanje pričakovanih škodljivih posledic ob morebitni realizaciji takšnega incidenta. Zavezancu se pisni odpravek ustne odločbe vroči čim prej, vendar najkasneje v roku 48 ur po ustni odločbi.

(5) Ukrepi, izdani na podlagi prejšnjega odstavka, se določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz prejšnjega odstavka. Pritožba zoper odločbo ne zadrži njene izvršitve.

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

23. člen
(obveščanje javnosti)

Če je v zvezi s sprejetimi ukrepi iz 21. ali prejšnjega člena tega zakona potrebno tudi obveščanje javnosti, pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, pripravi sporočilo za javno objavo, ki ga mediji smejo objaviti le v nespremenjeni obliki.

24. člen
(kibernetska obramba)

(1) Kibernetsko obrambo usklajujejo in izvajajo pristojni nacionalni organ, nacionalni CSIRT in CSIRT organov državne uprave ter ministrstvo, pristojno za obrambo, policija, Slovenska obveščevalno-varnostna agencija (v nadaljnjem besedilu: SOVA) in drugi nacionalni organi skladno s svojimi pristojnostmi pri zagotavljanju nacionalne varnosti.

(2) Pristojni organi iz prejšnjega odstavka zagotavljajo ustrezne zmogljivosti kibernetske obrambe v svojem kibernetskem prostoru. Pri tem ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za zunanje zadeve, ter policija in SOVA stalno spremljajo stanje in odzive na dogodke v kibernetskem prostoru.

(3) Za namen kibernetske obrambe organi iz prvega in prejšnjega odstavka na različnih ravneh izvajajo usklajene organizacijske, logično-tehnične, tehnične in administrativne ukrepe ter dejavnosti za zagotavljanje celovite informacijske varnosti skladno s svojimi pristojnostmi.

(4) Namen iz prejšnjega odstavka se uresničuje tudi z vključevanjem organov iz prvega in drugega odstavka tega člena v mednarodne varnostne povezave in njihovim aktivnim sodelovanjem v teh povezavah ter prek drugih oblik multilateralnega in bilateralnega sodelovanja.

VIII. Seznami

25. člen
(vodenje in vsebina seznamov)

(1) Pristojni nacionalni organ za namen sodelovanja z zavezanci vodi seznam kontaktnih podatkov, ki vsebuje:
- matično in davčno številko ter klasifikacijo dejavnosti zavezanca,
- naziv, naslov, telefonsko številko ter elektronski naslov zavezanca,
- ime in priimek, številko telefona in elektronski naslov kontaktne osebe zavezanca ter njenega namestnika iz 10. člena tega zakona.

(2) Do seznama iz prejšnjega odstavka imata v delu, ki se nanaša na zavezance iz njune pristojnosti, dostop tudi nacionalni CSIRT in CSIRT organov državne uprave.

(3) Pristojni nacionalni organ za namen preprečevanja in odzivanja na incidente ter kibernetske napade vodi skupen seznam incidentov in kibernetskih napadov, ki vsebuje:
- poročilo o incidentu ali kibernetskem napadu z identifikacijskimi podatki zavezanca in informacijskega sistema ali omrežja, kjer se je incident ali napad zgodil, ter podatki o incidentu ali napadu,
- podatke o viru incidenta ali napada,
- potek obveščanja preostalih pristojnih organov in postopek obveščanja drugih morebiti prizadetih subjektov,
- potek reševanja incidenta ali napada in končni rezultat ter ukrepe, sprejete za preprečitev ponavljanja oziroma za zmanjšanje tveganja pojava incidenta ali napada.

(4) Nacionalni CSIRT in CSIRT organov državne uprave za namen preprečevanja in odzivanja na incidente ter kibernetske napade vodita seznam incidentov in kibernetskih napadov s podatki iz prejšnjega odstavka za incidente, ki jih obravnavata.

(5) Pristojni nacionalni organ za namen ustrezne določitve izvajalcev bistvenih storitev in organov državne uprave vodi tudi seznam bistvenih storitev ter seznam informacijskih sistemov, delov omrežja in informacijskih storitev organov državne uprave, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

(6) Pristojni nacionalni organ in nacionalni CSIRT ter CSIRT organov državne uprave na podlagi podatkov iz tretjega in četrtega odstavka tega člena za statistične namene in namene seznanjanja javnosti dvakrat letno pripravijo anonimizirane informacije, ki jih tudi javno objavijo na svojih spletnih straneh.

IX. Organizacija nacionalnega sistema informacijske varnosti

26. člen
(strategija informacijske varnosti)

Vlada sprejme strategijo informacijske varnosti (v nadaljnjem besedilu: strategija), ki predstavlja okvir za izvedbo ukrepov za vzpostavitev učinkovitega nacionalnega sistema zagotavljanja informacijske varnosti. S tem namenom opredeljuje strateške cilje ter ukrepe politike in regulativne ukrepe, ki morajo zajemati vsaj področja iz drugega odstavka 5. člena, digitalne storitve iz 8. člena in storitve organov državne uprave iz 9. člena tega zakona. Pri tem obravnava zlasti:

1. cilje in prednostne naloge strategije;
2. okvir upravljanja za dosego ciljev in prednostnih nalog strategije, vključno z vlogami in odgovornostmi državnih organov in drugih ustreznih deležnikov;
3. opredelitev ukrepov v zvezi s pripravljenostjo, odzivanjem in ponovno vzpostavitvijo informacijske varnosti, vključno s sodelovanjem med javnim in zasebnim sektorjem;
4. opredelitev programov izobraževanja, ozaveščanja in usposabljanja v zvezi s strategijo;
5. opredelitev načrtov raziskav in razvoja v zvezi s strategijo;
6. načrt ocene tveganja za prepoznavanje tveganj;
7. seznam različnih subjektov, vključenih v izvajanje strategije.

27. člen
(pristojni nacionalni organ)

(1) Pristojni nacionalni organ je organ v sestavi ministrstva, pristojnega za informacijsko družbo.

(2) Pristojni nacionalni organ poleg drugih nalog, določenih s tem zakonom, izvaja še naslednje naloge:

1. koordinira delovanje 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 prisotnosti;
5. sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, predvsem z nacionalnim CSIRT in CSIRT organov državne uprave, z varnostno-operativnimi centri, z regulatorji oziroma nadzorniki področij iz drugega odstavka 5. člena, z Agencijo za komunikacijska omrežja in storitve Republike Slovenije, z Informacijskim pooblaščencem in z organi kazenskega pregona ter s ponudniki varnostnih rešitev;

6. zavezance ozavešča o pomembnosti prijave incidenta z vsemi znaki kaznivega dejanja, ki se preganja po uradni dolžnosti, organom kazenskega pregona, skladno s Kazenskim zakonikom;
7. koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za dvig zavedanja javnosti o informacijski varnosti;
8. spodbuja in podpira raziskave in razvoj na področju informacijske varnosti;
9. izvaja testiranja informacijsko-komunikacijskih tehnologij na področju informacijske varnosti;
10. skrbi za pripravo in izvajanje strategije;
11. izdela nacionalni načrt odzivanja na incidente ob upoštevanju strategije, načrtov nacionalnega CSIRT in CSIRT organov državne uprave, drugih pristojnih organov ter varnostne dokumentacije zavezancev;
12. pregleduje ustreznost določitve izvajalcev bistvenih storitev in organov državne uprave vsaj vsaki dve leti ter vladi lahko predlaga posodobitev določitev;
13. za namene pregleda Direktive 2016/1148/ES Evropsko komisijo vsaj vsaki dve leti obvešča o ukrepih za določitev storitev izvajalcev bistvenih storitev, njihovem številu ter pomenu, o seznamu bistvenih storitev ter pragih za določitev ustrezne ravni opravljanja storitev izvajalcev bistvenih storitev glede na število uporabnikov ali glede na pomen zadevnega izvajalca bistvenih storitev;
14. je enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU ter z mrežo skupin CSIRT in s skupino za sodelovanje, v katero prispeva svojega predstavnika;
15. izpolnjuje druge obveznosti obveščanja Evropske komisije in skupine za sodelovanje, obveznosti obveščanja in notifikacije preostalih mednarodnih organizacij;
16. izvaja druge naloge mednarodnega sodelovanja.

28. člen
(nacionalni CSIRT)

(1) Nacionalni CSIRT je odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri javnem zavodu Akademska in raziskovalna mreža Slovenije.

(2) Nacionalni CSIRT poleg drugih nalog, določenih s tem zakonom, izvaja še naslednje naloge:
1. zavezancem, za katere je pristojen, nudi metodološko podporo, pomoč in sodelovanje ob pojavitvi incidenta;
2. sprejema podatke o tveganjih in ranljivostih na področju informacijske varnosti, jih posreduje skrbnikom prizadetih sistemov in objavlja opozorila;
3. sodeluje v mreži skupin CSIRT, lahko pa tudi v drugih mednarodnih mrežah za sodelovanje;
4. sodeluje s skupinami CSIRT in varnostno-operativnimi centri v Republiki Sloveniji ter skupinami CSIRT v drugih državah članicah EU;
5. izvaja ozaveščanje uporabnikov na področju informacijske varnosti;
6. objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti;
7. sodeluje s pristojnim nacionalnim organom in mu na poziv nudi informacije o izvajanju svojih pristojnosti na podlagi tega zakona.

(3) Nacionalni CSIRT izpolnjuje zahteve glede visoke stopnje razpoložljivosti svojih storitev, varnosti svojih poslovnih prostorov ter neprekinjenega poslovanja skladno z Direktivo 2016/1148/ES.

29. člen

(CSIRT organov državne uprave)

(1) Naloge CSIRT organov državne uprave izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave.

(2) CSIRT organov državne uprave poleg drugih nalog, določenih s tem zakonom, izvaja še naslednje naloge:
- sprejema, obravnava in ocenjuje priglasitve incidentov, prejete od zavezancev, za katere je pristojen, ter te podatke evidentira, hrani in varuje;
- zavezancem, za katere je pristojen, nudi metodološko podporo, pomoč in sodelovanje ob pojavu incidenta;
- sodeluje z nacionalnim CSIRT in s pristojnim nacionalnim organom ter jima na poziv na varen način nudi informacije o izvajanju svojih pristojnosti na podlagi tega zakona;
- objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti organov državne uprave.

30. člen
(sodelovanje na nacionalni ravni)

(1) Nacionalni CSIRT in CSIRT organov državne uprave pristojnemu nacionalnemu organu četrtletno posredujeta poročilo o izvajanju svojih nalog.

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

X. Nadzor

31. člen
(pristojnost, postopek in pravna sredstva)

(1) Nadzor nad izvajanjem določb tega zakona, na njegovi podlagi sprejetih predpisov in nad izvajanjem upravnih odločb, izdanih na podlagi četrtega odstavka 21. člena in četrtega odstavka 22. člena tega zakona, opravljajo inšpektorji za informacijsko varnost pristojnega nacionalnega organa (v nadaljnjem besedilu: inšpektor).

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

(3) Inšpektor o obravnavi zadev iz prvega odstavka tega člena, katerih posledica je kršitev varstva osebnih podatkov, obvešča Informacijskega pooblaščenca. Za namen pravočasnega ukrepanja v smeri zagotavljanja odprave kršitev varstva osebnih podatkov inšpektor Informacijskega pooblaščenca obvešča tudi v primerih suma kršitve varstva osebnih podatkov.

(4) Tožba v upravnem sporu zoper dokončno odločbo, izdano v postopkih nadzora po tem zakonu, se vloži na sedežu Upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.

32. člen
(nadzor nad izvajalci bistvenih storitev)

(1) Inšpektor nadzira, ali izvajalci bistvenih storitev izpolnjujejo svoje obveznosti iz prvega in petega odstavka 10. člena, iz 11. člena, iz prvega, drugega in petega odstavka 12. člena, iz prvega in drugega odstavka 13. člena, iz šestega odstavka 14. člena tega zakona ter iz odločb, izdanih na podlagi četrtega odstavka 21. člena in četrtega odstavka 22. člena tega zakona, ter na njihovi podlagi določene ukrepe za varnost omrežij in informacijskih sistemov.

(2) Inšpektor lahko od izvajalcev bistvenih storitev zahteva, da predložijo informacije, potrebne za oceno varnosti njihovih omrežij in informacijskih sistemov, vključno z dokumentiranimi varnostnimi pravili, ter dokaze o učinkovitem izvajanju varnostnih pravil. Kadar inšpektor zahteva takšne informacije ali dokaze, navede namen te zahteve in opredeli, katere dodatne informacije so potrebne. Na podlagi navedenih informacij lahko izvajalcem bistvenih storitev izreka ukrepe za odpravo ugotovljenih pomanjkljivosti.

(3) Za dokaz o učinkovitem izvajanju varnostnih pravil iz prejšnjega odstavka se šteje ocena varnosti omrežij in informacijskih sistemov, ki jo je izvajalec bistvenih storitev pripravil skupaj s pristojnim nacionalnim organom, ali ocena varnosti, ki jo je za izvajalca bistvenih storitev pripravil kvalificiran revizor.

33. člen
(nadzor nad ponudniki digitalnih storitev)

(1) Inšpektor nadzira, ali ponudniki digitalnih storitev, za katere je pristojen skladno s prvim ali drugim odstavkom 15. člena tega zakona, izpolnjujejo svoje obveznosti iz prvega, drugega in tretjega odstavka 14. člena tega zakona ter iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona.

(2) Če so inšpektorju predloženi dokazi, da ponudnik digitalnih storitev ne izpolnjuje katerekoli obveznosti iz prejšnjega odstavka, izda odločbo, s katero mu naloži odpravo pomanjkljivosti.

(3) Dokaze iz prejšnjega odstavka lahko predložijo tudi pristojni organi drugih držav članic EU, v katerih se storitev izvaja, ki lahko tudi predlagajo sprejem nadzornih ukrepov iz prejšnjega odstavka.

(4) Inšpektor lahko od ponudnikov digitalnih storitev tudi zahteva, da predložijo informacije in dokaze, potrebne za oceno varnosti njihovega omrežja in informacijskih sistemov, vključno z dokumentiranimi varnostnimi pravili.

(5) Inšpektor v postopkih nadzora iz prvega odstavka tega člena po potrebi sodeluje s pristojnimi organi nadzora v drugih državah članicah EU, če ima ponudnik digitalnih storitev svoja omrežja in informacijske sisteme v eni ali več drugih državah članicah EU. Takšno sodelovanje zajema izmenjavo informacij med zadevnimi organi nadzora.

(6) Informacije in podatki iz prejšnjega odstavka, ki so zaupni, se izmenjujejo, če je to potrebno za uporabo Direktive 2016/1148/ES oziroma za izvajanje tega zakona. Izmenjava je omejena na obseg, ki je primeren in nujen glede na namen iz prejšnjega odstavka ter mora ohraniti zaupnost posredovanih informacij in podatkov.

34. člen
(nadzor nad organi državne uprave)

(1) Inšpektor nadzira, ali organi državne uprave izpolnjujejo svoje obveznosti iz prvega in drugega odstavka 16. člena, iz prvega, drugega in petega odstavka 17. člena, iz

prvega in drugega odstavka 18. člena tega zakona ter iz odločb, izdanih na podlagi četrtega odstavka 21. člena in četrtega odstavka 22. člena tega zakona, ter na njihovi podlagi določene ukrepe za varnost omrežij in informacijskih sistemov.

(2) Inšpektor lahko od državnih organov zahteva, da predložijo informacije, potrebne za oceno varnosti njihovih omrežij in informacijskih sistemov oziroma informacijskih storitev, vključno z dokumentiranimi varnostnimi pravili, ter dokaze o učinkovitem izvajanju varnostnih pravil. Kadar inšpektor zahteva takšne informacije ali dokaze, navede namen te zahteve in opredeli, katere dodatne informacije so potrebne.

(3) Za dokaz o učinkovitem izvajanju varnostnih pravil iz prejšnjega odstavka se šteje ocena varnosti omrežij in informacijskih sistemov, ki jo je organ državne uprave pripravil skupaj s pristojnim nacionalnim organom, ali ocena varnosti, ki jo je za organ državne uprave pripravil kvalificiran revizor.

(4) Inšpektor lahko na podlagi ocene varnosti iz prejšnjega odstavka organov državne uprave izreka ukrepe za odpravo ugotovljenih pomanjkljivosti.

35. člen
(posebni ukrep)

Ne glede na določbe zakona, ki ureja inšpekcijski nadzor, lahko inšpektor zavezancem le v skrajnem primeru in upoštevaje pomen področij iz drugega odstavka 5. člena tega zakona oziroma njihovega sistema ter dejavnosti, prepove uporabo tega sistema ali njegovega dela, dokler ni ugotovljena pomanjkljivost odpravljena in če s tem ukrepom ni ogrožena zanesljivost oskrbe na posameznem področju oziroma zagotavljanje njihovih storitev.

XI. Kazenske določbe

36. člen
(višina globe v hitrem prekrškovnem postopku)

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

37. člen
(prekrški izvajalca bistvenih storitev)

(1) Z globo od 500 do 10.000 eurov se kaznuje pravna oseba, z globo od 10.000 do 50.000 eurov pa pravna oseba, ki se po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, če:

1. ne izpolni obveznosti iz prvega ali petega odstavka 10. člena tega zakona,
2. ne izpolni obveznosti iz 11. člena tega zakona,
3. ne izpolni obveznosti iz prvega, drugega ali petega odstavka 12. člena tega zakona,
4. ne izpolni obveznosti iz prvega ali drugega odstavka 13. člena tega zakona,
5. ne izpolni obveznosti iz šestega odstavka 14. člena tega zakona,
6. ne izpolni obveznosti iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona,
7. ne izpolni obveznosti iz odločbe, izdane na podlagi četrtega odstavka 22. člena tega zakona.

(2) Z globo od 500 do 10.000 eurov se kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če stori prekršek iz prejšnjega odstavka.

(3) Z globo od 200 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, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, ki je izvajalec bistvenih storitev po tem zakonu, če stori prekršek iz prvega odstavka tega člena.

38. člen
(prekrški ponudnika digitalnih storitev)

(1) Z globo od 500 do 10.000 eurov se kaznuje pravna oseba, z globo od 10.000 do 50.000 eurov pa pravna oseba, ki se po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, če:
- ne izpolni obveznosti iz prvega, drugega ali tretjega odstavka 14. člena tega zakona,
- ne izpolni obveznosti iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona.

(2) Z globo od 500 do 10.000 eurov se kaznuje samostojni podjetnik posameznik, če stori prekršek iz prejšnjega odstavka.

(3) Z globo od 200 do 2.000 eurov se kaznuje odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika, ki je ponudnik digitalnih storitev po tem zakonu, če stori prekršek iz prvega odstavka tega člena.

39. člen
(prekrški organov državne uprave)

Z globo od 200 do 2.000 eurov se kaznuje odgovorna oseba v organu državne uprave, če slednji:
- ne izpolni obveznosti iz 16. člena tega zakona,
- ne izpolni obveznosti iz prvega, drugega ali petega odstavka 17. člena tega zakona,
- ne izpolni obveznosti iz prvega ali drugega odstavka 18. člena tega zakona,
- ne izpolni obveznosti iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona,
- ne izpolni obveznosti iz odločbe, izdane na podlagi četrtega odstavka 22. člena tega zakona.

XII. Prehodne določbe

40. člen
(začetek delovanja pristojnega nacionalnega organa)

(1) Pristojni nacionalni organ začne z delovanjem najkasneje do 1. januarja 2020.

(2) Do pričetka delovanja pristojnega nacionalnega organa njegove naloge opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljnjem besedilu: UVTP) skladno s tem zakonom, razen nalog upravnega odločanja in nadzora, ki jih opravlja ministrstvo, pristojno za informacijsko družbo.

(3) Pristojni nacionalni organ z dnem začetka delovanja od UVTP prevzame naloge, arhive in dokumentacijo, ki se nanašajo na informacijsko varnost, ter javne uslužbence, pravice proračunske porabe, opremo in druge zbirke podatkov oziroma evidence iz prevzetega delovnega področja.

(4) Vlada uskladi Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uradni list RS, št. 6/02 in 17/17) s tem zakonom v treh mesecih od njegove uveljavitve.

41. člen
(delovanje drugih pristojnih organov)

(1) Nacionalni CSIRT začne z delovanjem po tem zakonu 1. januarja 2019.

(2) CSIRT organov državne uprave se vzpostavi na ministrstvu, pristojnem za upravljanje informacijsko-komunikacijskih sistemov državne uprave, 1. januarja 2019.

(3) Do vzpostavitve CSIRT organov državne uprave njegove naloge glede obravnave incidentov izvaja nacionalni CSIRT.

42. člen
(izdaja podzakonskih predpisov in strategije)

(1) Vlada uskladi Uredbo o organih v sestavi ministrstev (Uradni list RS, št. 35/15, 62/15, 84/16, 41/17 in 53/17) s tem zakonom v treh mesecih od njegove uveljavitve.

(2) Podzakonski predpisi iz prvega odstavka 6. člena, četrtega odstavka 7. člena, tretjega odstavka 12. člena in tretjega odstavka 17. člena tega zakona se sprejmejo v šestih mesecih od uveljavitve tega zakona.

(3) Vlada sprejme strategijo iz 26. člena tega zakona v enem letu od uveljavitve tega zakona.

43. člen
(prehodno obdobje)

(1) Vlada določi posamezne izvajalce bistvenih storitev iz drugega in tretjega odstavka 6. člena tega zakona v šestih mesecih od uveljavitve uredb iz prvega odstavka 6. člena in iz četrtega odstavka 7. člena tega zakona.

(2) Izvajalec bistvenih storitev mora izpolniti varnostne zahteve in zahteve za priglasitev incidentov iz 11., 12. in 13. člena tega zakona skladno s tem zakonom v šestih mesecih od njegove določitve iz prejšnjega odstavka.

(3) Ponudnik digitalnih storitev mora izpolniti varnostne zahteve in zahteve za priglasitev incidentov iz 14. člena tega zakona skladno s tem zakonom v devetih mesecih od uveljavitve tega zakona.

(4) Vlada določi organe državne uprave skladno z 9. členom tega zakona v devetih mesecih od uveljavitve tega zakona.

(5) Organi državne uprave morajo izpolniti varnostne zahteve in zahteve za priglasitev incidentov iz 16., 17. in 18. člena tega zakona skladno s tem zakonom v dvanajstih mesecih od njihove določitve iz prejšnjega odstavka.

XIII. Končna določba

44. člen
(začetek veljavnosti)

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

Št. 011-02/18-4/13
Ljubljana, dne 17. aprila 2018
EPA 2594-VII

Državni zbor
Republike Slovenije
dr. Milan Brglez l.r.