# Zakon o informacijski varnosti

## I. Splošne določbe

1. člen

(vsebina zakona)

Ta zakon ureja ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji (v nadaljnjem besedilu: RS), ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah, zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti ter ureja zagotavljanje informacijske varnosti in kibernetske obrambe v RS. Določa minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona. Prav tako ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa, enotne kontaktne točke in posameznih skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljnjem besedilu: CSIRT) na področju zagotavljanja informacijske varnosti in kibernetske obrambe ter ureja posamezna področja varovanja in posredovanja informacij, podatkov ter zaščite le-teh v opredeljenih omrežjih in informacijskih sistemih.

2. člen

(namen in področje uporabe zakona)

(1) Namen zakona je zagotovitev visoke ravni varnosti omrežij in informacijskih sistemov v RS, 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 RS prenaša Direktiva 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 (Direktiva NIS) (UL L št. 194 z dne 19. 7. 2016, str. 1- 30).

(3) Ta zakon se smiselno uporablja tudi za omrežja in informacijske sisteme, ki so akreditirani za obravnavanje tajnih podatkov v skladu z zakonom in predpisi, ki urejajo področje tajnih podatkov.

(4) Ta zakon se ne uporablja za operaterje, 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.

(5) Ta zakon ne posega v zakonodajo s področja urejanja temeljnih državnih funkcij, zlasti za zaščito nacionalne varnosti, vključno z ukrepi za zaščito informacij, katerih razkritje bi bilo v nasprotju s temeljnimi interesi varnosti države, ter za ohranitev javnega reda in miru, predvsem za omogočanje preiskovanja, odkrivanja in pregona kaznivih dejanj.

(6) Ta zakon ne posega v zakonodajo s področja kritične infrastrukture, s področja kazenskega urejanja boja proti spolni zlorabi otrok in spolnem izkoriščanju otrok ter otroške pornografije ter s področja kazenskega urejanja napadov na informacijske sisteme.

(7) Ob upoštevanju 346. člena Pogodbe o delovanju EU se informacije na podlagi tega zakona, ki so zaupne narave v skladu s predpisi EU in nacionalnimi predpisi, z Evropsko komisijo in drugimi ustreznimi organi izmenjajo le, če je takšna izmenjava potrebna za uporabo tega zakona. Izmenjava informacij je omejena na obseg, ki je ustrezen in sorazmeren glede na namen te izmenjave. Pri takšni izmenjavi informacij se ohranijo zaupnost zadevnih informacij ter zaščitijo varnost in poslovni interesi izvajalcev bistvenih storitev in ponudnikov digitalnih storitev.

(8) Če neposredno uporabljivi predpisi Evropske Unije (v nadaljnjem besedilu: EU) ali področni nacionalni predpisi, ki prenašajo predpise EU, zahtevajo, da izvajalec bistvenih storitev ali ponudnik digitalnih storitev zagotovi varnost svojih omrežij in informacijskih sistemov ali priglasi incidente, se uporabljajo zadevne določbe prej navedene področne zakonodaje, če so takšne zahteve po učinku vsaj enakovredne obveznostim iz tega zakona.

3. člen

(obdelava osebnih podatkov in izmenjava informacij)

Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno z zakonom, ki ureja varstvo osebnih podatkov.

4. člen

(pomen izrazov)

(1) 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;

(2) Digitalna infrastruktura pomeni stičišča omrežij, register domenskih imen najvišje ravni in ponudnika storitev sistema domenskih imen najvišje ravni;

(3) Digitalna storitev pomeni katero koli storitev informacijske družbe ali katero koli 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. Za potrebe tega zakona so digitalne storitve storitve spletne tržnice, spletnega iskalnika in računalništva v oblaku;

(4) Incident pomeni vsak dogodek, ki ima dejanski negativen učinek na varnost omrežij in informacijskih sistemov;

(5) Informacijska varnost pomeni zaščito, varovanje in obrambo omrežij in informacijskih sistemov ter informacij pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti;

(6) Informacijsko okolje pomeni skupek družbenih omrežij in kibernetskega prostora, vključno s podatki;

(7) Izvajalec bistvenih storitev pomeni javni ali zasebni subjekt, ki spada v katerega od sektorjev,

navedenih v 5. členu tega zakona in izpolnjuje merila, določena v 6. členu tega zakona ter dodatna sektorska merila, določena s posebnim predpisom;

(8) Kibernetska grožnja pomeni možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja ali sistema;

(9) Kibernetska obramba predstavlja celoto tehničnih in netehničnih ukrepov in dejavnosti, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju;

(10) Kibernetska varnost pomeni sposobnost zaščititi, varovati ali braniti kibernetski prostor pred kibernetskimi napadi;

(11) Kibernetski napad predstavlja napad z namenom zlonamernega uničevanja, izpostavljanja, nadzorovanja ali spreminjanja, onemogočanja, zbiranja in oviranja katerega koli dela omrežja oziroma informacijskih sistemov, vključno z informacijami, ki so bistvenega pomena za nemoteno delovanje države;

(12) Kibernetski prostor predstavlja globalno omrežje informacijske tehnologije, elektronsko-komunikacijskih omrežij in sistemov za računalniško obdelavo;

(13) Ključni informacijski sistemi so vsi informacijski sistemi subjekta, ki so bistvenega pomena za neprekinjeno izvajanje storitve;

(14) Krmilni informacijski sistemi so informacijski sistemi, ki omogočajo izvajanje pravilnih postopkov in izvajajo ustrezno sosledje delovanja ključnih informacijskih sistemov subjekta;

(15) Mikro, majhna in srednje velika podjetja imajo za potrebe tega zakona enak pomen kot ga določa priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, majhnih in srednje velikih podjetij ne glede na to, ali dejavnost opravljajo v obliki gospodarske družbe ali kot samostojni podjetnik posameznik;

(16) Mreža skupin CSIRT je povezava, v kateri sodelujejo skupine CSIRT iz držav članic in CERT-EU. Evropska komisija v njej sodeluje kot opazovalka;

(17) Nadzorni informacijski sistemi so informacijski sistemi, ki skrbijo za izvajanje nadzorstvene funkcije vseh informacijskih sistemov subjekta;

(18) Obvladovanje incidentov pomeni vse postopke, ki podpirajo odkrivanje, analizo in zajezitev incidentov ter odzivanje nanje;

(19) Omrežje in informacijski sistem pomeni:

a) elektronsko komunikacijsko omrežje pomeni prenosne sisteme in, kjer je primerno, komutacijsko ali usmerjalno 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, omrežji, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kabelske televizije, ne glede na vrsto prenesenih informacij;

b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali
c) digitalne podatke, ki jih elementi iz točk (a) in (b) shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;

(20) Ponudnik digitalnih storitev pomeni vsako pravno osebo, ki zagotavlja digitalno storitev;

(21) Ponudnik storitev sistema domenskih imen pomeni subjekt, ki zagotavlja storitve sistema domenskih imen na internetu;

(22) Predstavnik pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki je izrecno določena, da deluje v imenu ponudnika digitalnih storitev, ki nima sedeža v Uniji, in s katero lahko agencija ali skupina CSIRT vzpostavi stik namesto s ponudnikom digitalnih storitev, kar zadeva obveznosti tega ponudnika digitalnih storitev na podlagi tega zakona;

(23) Register domenskih imen najvišje ravni pomeni subjekt, ki upravlja in izvaja registracijo imen internetnih domen v okviru določene domene najvišje ravni;

(24) Revizijska sled je nespremenljiva sled oziroma niz podatkov, ki se je zgodila v informacijskem sistemu, z natančnim časovnim zapisom v obliki dnevniškega zapisa, ki omogoča natančni pregled vseh zapisov povezanih z vsemi dogodki in vsemi shranjenimi informacijami od nastanka podatka ali informacije dalje do trenutnega stanja;

(25) Sistem domenskih imen pomeni hierarhičen porazdeljen sistem dodeljevanja imen v omrežju, ki posreduje poizvedbe za domenska imena;

(26) Skupina za sodelovanje je skupina, ki jo sestavljajo predstavniki držav članic, Evropske komisije in Agencije Evropske unije za varnost omrežij in informacij (agencija ENISA);

(27) Specifikacija pomeni dokument, ki predpisuje tehnične zahteve, ki jih mora izpolniti proizvod, proces, storitev ali sistem;

(28) Spletna tržnica pomeni digitalno storitev, ki omogoča potrošnikom (vsaka fizična oseba, ki deluje za namene zunaj okvira svoje trgovske, poslovne, obrtne ali poklicne dejavnosti) in/ali 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), da na spletišču spletne tržnice ali spletišču trgovca, ki uporablja računalniške storitve spletne tržnice, s trgovci sklenejo pogodbe o spletni prodaji ali pogodbe o spletnih storitvah;

(29) Spletni iskalnik pomeni digitalno storitev, ki uporabnikom na podlagi poizvedbe na katero koli temo 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;

(30) Standard pomeni tehnično specifikacijo, ki jo je sprejel priznan organ za standardizacijo za večkratno ali stalno uporabo;

(31) Stičišče omrežij pomeni omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih avtonomnih sistemov, predvsem zaradi izmenjave internetnega prometa; stičišče

omrežij zagotavlja medsebojno povezavo le avtonomnih sistemov; stičišče omrežij omogoča izmenjavo internetnega prometa med katerima koli sodelujočima avtonomnima sistemoma, brez prehoda prek tretjega avtonomnega sistema, prav tako pa ne spreminja takšnega prometa ali kako drugače posega vanj;

(32) Storitev računalništva v oblaku pomeni digitalno storitev, ki omogoča dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov;

(33) Strategija kibernetske varnosti je nacionalna strategija za varnost omrežij in informacijskih sistemov in pomeni okvir s strateškimi cilji in prednostnimi nalogami na področju varnosti omrežij in informacijskih sistemov v RS;

(34) Tveganje pomeni vsako razumno določljivo okoliščino ali dogodek, ki ima lahko negativen učinek na varnost omrežij in informacijskih sistemov;

(35) Varnost omrežij in informacijskih sistemov pomeni 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 dostopne.

## II. Zavezanci

5. člen

(zavezanci)

(1) Zavezanci po tem zakonu so:
- izvajalci bistvenih storitev in
- ponudniki digitalnih storitev.

(2) Izvajalci bistvenih storitev so subjekti, ki delujejo v naslednjih sektorjih:
- energija,
- digitalna infrastruktura,
- oskrba s pitno vodo in njena distribucija,
- zdravstvo,
- promet,
- bančništvo,
- infrastruktura finančnega trga,
- zagotavljanje delovanja ključnih delov nacionalnega varnostnega sistema ter državnih organov in samoupravnih lokalnih skupnosti.

(3) Izvajalci bistvenih storitev, ki delujejo v sistemu varstva pred naravnimi nesrečami, obrambe in notranje varnosti so neposredno odgovorni pristojnim organom glede na njihove pristojnosti, ki po tem zakonu opravljajo tako naloge zavezanca kot naloge pristojnega organa.

(4) Vlada RS (v nadaljnjem besedilu: vlada) seznam storitev, ki jih izvajajo izvajalci bistvenih storitev predpiše v uredbi.

(5) Vlada na predlog pristojnega nacionalnega organa s sklepom določi izvajalce bistvenih storitev, na podlagi meril iz 6. člena tega zakona. Kadar izvajalec zagotavlja storitev v RS in še kateri drugi državi članici, se te države članice za namen določitve izvajalcev posvetujejo med seboj. To posvetovanje se opravi pred sprejetjem sklepa o določitvi.

(6) Pristojni nacionalni organ vodi seznam bistvenih storitev in seznam izvajalcev bistvenih storitev.

(7) Pristojni nacionalni organ pisno obvesti zavezance o njihovem statusu, skupaj z navedbo pristojne skupine CSIRT za priglasitev incidentov.

6. člen

(merila - metodologija)

(1) Pri določitvi izvajalcev bistvenih storitev iz prvega odstavka 5. člena tega zakona se upošteva naslednja merila:
- subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih in/ali gospodarskih dejavnosti;
- zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov ter
- 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 naslednji medsektorski dejavniki:
- število uporabnikov, ki so odvisni od storitve zadevnega subjekta;
- odvisnost drugih sektorjev iz drugega odstavka 5. člena tega zakona od storitve tega subjekta;
- stopnjo in trajanje vpliva, ki bi ga incidenti lahko imeli na gospodarske in družbene dejavnosti ali javno varnost;
- tržni delež tega subjekta;
- geografsko razširjenost, kar zadeva območje, ki bi ga incident lahko prizadel;
- pomen subjekta za ohranitev zadostne ravni storitve ob upoštevanju razpoložljivosti alternativnih načinov za zagotavljanje zadevne storitve.

(3) Pri odločanju, ali bi incident imel pomemben negativen vpliv, se upoštevajo tudi sektorski dejavniki.

(4) Pri določitvi ponudnikov digitalnih storitev iz prvega odstavka 5. člena tega zakona se uporabijo enotna merila, sprejeta na ravni EU.

(5) Vlada metodologijo za določitev izvajalcev bistvenih storitev, ki upošteva tudi sektorske dejavnike, podrobneje predpiše v uredbi. Pri tem upošteva tudi priporočila skupine za sodelovanje za usklajen pristop za določitev izvajalcev bistvenih storitev v EU.

7. člen

(določitev kontaktne osebe za informacijsko varnost zavezanca)

(1) Zavezanci določijo in pooblastijo kontaktno osebo za informacijsko varnost in njenega namestnika ter kontaktne podatke posredujejo pristojnemu nacionalnemu organu v 15 dneh od prejema pisnega obvestila pristojnega nacionalnega organa iz sedmega odstavka 5. člena tega zakona.

(2) O spremembi kontaktnih podatkov so zavezanci dolžni v roku 15 delovnih dni po nastali spremembi obvestiti pristojni nacionalni organ.

## III. Informacijska varnost izvajalcev bistvenih storitev

8. člen

(varnostne zahteve in priglasitev incidentov)

(1) Izvajalci bistvenih storitev skladno z metodologijo, predpisano z uredbo iz petega odstavka 6. člena tega zakona, določijo svoje ključne, krmilne in nadzorne informacijske sisteme in dele omrežja, s katerimi zagotavljajo izvajanje svojih storitev.

(2) Izvajalci bistvenih storitev morajo izvesti analizo, oceno in vrednotenje tveganj ter na tej osnovi pripraviti in izvesti potrebne ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri svojih dejavnostih.

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

(4) Izvajalci bistvenih storitev pristojnemu 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. Priglasitev ne sme nalagati priglasitelju dodatne odgovornosti. Pri določitvi pomembnosti vpliva incidenta zlasti upoštevajo:
   - število uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvene storitve,
   - trajanje incidenta in
   - geografsko razširjenost, kar zadeva območje, na katerega vpliva incident.

(5) Ne glede na določbe prejšnjega odstavka je priglasitelj v primeru incidenta z znaki kaznivega dejanja dolžan takoj o tem obvestiti pristojne organe kazenskega pregona.

(6) Priglasitelj mora ob prijavi incidenta poskrbeti za ustrezno zavarovanje podatkov revizijskih sledi.

(7) Pristojni CSIRT o incidentu, ki bi lahko imel večji medsektorski vpliv, oziroma bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti RS, nemudoma obvesti druge skupine CSIRT, pristojni nacionalni organ, policijo ter po potrebi tudi Nacionalni center za krizno upravljanje.

(8) Postopek obveščanja pristojnih organov s strani skupin CSIRT in pristojnega nacionalnega organa glede poročanja o incidentih, ki imajo znake kaznivih dejanj in se preganjajo po uradni dolžnosti, se uredi z medsebojnim sporazumom.

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

(10) Če je mogoče, pristojni CSIRT izvajalcu bistvenih storitev, ki priglasi incident, predloži ustrezne informacije glede nadaljnjih ukrepov na podlagi njegove priglasitve, ki bi lahko prispevale k učinkovitemu obvladovanju incidenta.

(11) Pristojni nacionalni organ ali skupina CSIRT lahko po posvetovanju z izvajalcem bistvenih storitev, ki je priglasil incident, obvesti javnost o posameznih incidentih, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku.

(12) Pristojni organi, ki sodelujejo v okviru skupine za sodelovanje, lahko oblikujejo in sprejmejo smernice o okoliščinah, v katerih morajo izvajalci bistvenih storitev priglasiti incidente, vključno s parametri za določitev pomembnosti vpliva incidenta.

## IV. Informacijska varnost ponudnikov digitalnih storitev

9. člen

(varnostne zahteve in priglasitev incidentov)

(1) Ponudniki digitalnih storitev morajo izvesti analizo, oceno in vrednotenje tveganj ter na tej osnovi pripraviti in izvesti potrebne ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri svojih dejavnostih. Pri tem upoštevajo:
- varnost sistemov in zmogljivosti,
- obvladovanje incidentov,
- upravljanje neprekinjenega poslovanja,
- spremljanje, revidiranje in preizkušanje in
- 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 Uniji, da bi zagotovili neprekinjeno izvajanje teh storitev.

(3) Ponudniki digitalnih storitev pristojnemu CSIRT brez nepotrebnega odlašanja priglasijo vsak incident, ki ima pomemben vpliv na zagotavljanje njihovih storitev, ki jih ponujajo v Uniji. Priglasitev zajema informacije, na podlagi katerih je mogoče določiti pomembnost morebitnega čezmejnega vpliva. Priglasitev ne sme nalagati priglasitelju dodatne odgovornosti. Pri določitvi stopnje vpliva incidenta zlasti upoštevajo:
- 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 vpliva incident,
- v kakšnem obsegu je moteno delovanje storitve,
- obseg vpliva na gospodarske in družbene dejavnosti.

Obveznost priglasitve incidenta velja le, kadar ima ponudnik digitalnih storitev dostop do informacij, potrebnih za oceno vpliva incidenta.

(4) 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 priglasi vsak znaten vpliv na neprekinjeno izvajanje bistvenih storitev, ki je posledica incidenta, ki vpliva na ponudnika digitalnih storitev.

(5) Kadar je to ustrezno in zlasti če incident zadeva dve ali več držav članic, pristojni nacionalni organ ali pristojni CSIRT obvesti druge prizadete države članice. Pri tem zaščiti varnost in poslovne interese ponudnika digitalnih storitev ter zaupnost informacij, ki jih slednji zagotovi v svoji priglasitvi.

(6) Pristojni nacionalni organ ali pristojni CSIRT in, kadar je to ustrezno, organi ali skupine CSIRT drugih zadevnih držav članic lahko po posvetovanju z zadevnim ponudnikom digitalnih storitev obvestijo javnost o posameznih incidentih ali zahtevajo, da to stori ponudnik digitalnih storitev, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku, ali kadar je razkritje incidenta kako drugače v javnem interesu.

(7) Za ponudnike digitalnih storitev se ne uvedejo nikakršne nadaljnje varnostne zahteve ali zahteve glede priglasitve.

(8) Določbe členov iz poglavja IV ne veljajo za ponudnike digitalnih storitev, ki so mikro ali mala podjetja.

10. člen

(pristojnost in teritorialnost)

(1) Ponudnik digitalnih storitev, ki ima glavni sedež v RS sodi v pristojnost pristojnega nacionalnega organa. Za namene tega zakona se šteje, da ima ponudnik digitalnih storitev glavni sedež v RS, če ima v RS glavno upravo.

(2) Če ponudnik digitalnih storitev, ki nima sedeža v EU, v njej pa zagotavlja svoje storitve, določi sedež svojega predstavnika za EU v RS, kjer tudi zagotavlja svoje storitve, sodi v pristojnost pristojnega nacionalnega organa. Predstavnik zastopa ponudnika v zvezi z obveznostmi na podlagi tega zakona.

(3) Določitev predstavnika s strani ponudnika digitalnih storitev iz prejšnjega odstavka ne posega v sodne postopke, ki se lahko sprožijo proti samemu ponudniku digitalnih storitev.

(4) Če ima ponudnik digitalnih storitev glavni sedež ali predstavnika v eni državi članici EU, omrežja in informacijske sisteme pa v eni ali več drugih državah članicah EU, pristojni nacionalni organ v primeru, da je delovanje ponudnika digitalnih storitev kakorkoli povezano z RS, sodeluje glede na okoliščine primera s pristojnim organom iz države članice EU glavnega sedeža ponudnika ali

predstavnika ponudnika v EU oziroma z zadevnimi pristojnimi organi teh drugih držav članic EU, ki jim pomaga ali jih zaprosi za pomoč. Takšna pomoč in sodelovanje lahko zajemata izmenjavo informacij med zadevnimi pristojnimi organi in zahteve za sprejem ustreznih nadzornih ukrepov iz poglavja o inšpekcijskem nadzoru.

## V. Varnostna dokumentacija in varnostni ukrepi

11. člen

(varnostna dokumentacija)

Vsi zavezanci so dolžni za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov vzpostaviti in vzdrževati dokumentiran sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj:

- analizo obvladovanja tveganj z oceno sprejemljivega nivoja tveganj,
- politiko neprekinjenega poslovanja z načrtom upravljanja le-tega,
- seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja zavezanca ter pripadajočih podatkov, ki so bistvenega pomena za delovanje zavezanca,
- načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje,
- načrt odzivanja na incidente s protokolom obveščanja pristojnih organov ter pristojnega CSIRT.

12. člen

(varnostni ukrepi)

(1) Varnostni ukrepi, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe, upoštevajo tudi sektorske posebnosti, in morajo biti upoštevani v sistemu upravljanja varovanja informacij in sistemu upravljanja neprekinjenega poslovanja. Nanašajo se na zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov zavezancev.

(2) Med organizacijske ukrepe sodi najmanj:
- opredelitev varnostnih zahtev za dobavitelje,
- upravljanje sredstev,
- zagotavljanje visoke ravni integritete človeških virov,
- upravljanje prometa in komunikacij,
- dokumentiran razvoj in vzdrževanje informacijskih sistemov,
- obvladovanje incidentov.

(3) Med logično-tehnične ukrepe sodi najmanj:
- zagotavljanje fizičnega in tehničnega varovanja dostopov do prostorov, kjer se nahajajo ključni, krmilni ali nadzorni informacijski sistemi zavezanca,
- zagotavljanje mehanizmov za varnost v posamezni aplikativni programski opremi za izvajanje dejavnosti zavezanca,

- uporaba orodij za zbiranje in vrednotenje incidentov.

(4) Med tehnične ukrepe sodi najmanj:
- uporaba orodij, tehnik in mehanizmov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti komunikacijskih omrežij,
- uporaba orodij za preverjanje identitete uporabnikov,
- uporaba orodij za upravljanje pooblastil za dostop,
- uporaba orodij za zaščito pred zlonamernimi kodami,
- uporaba orodij za beleženje dejavnosti kritične informacijske infrastrukture in pomembnih informacijskih sistemov, njihovih uporabnikov in administratorjev,
- uporaba orodij za zaznavanje poskusov vdorov in preprečevanje incidentov,
- uporaba predpisanih šifrirnih mehanizmov in
- uporaba orodij za zagotavljanje ravni dostopnosti informacij.

(5) V kolikor je zavezanec po tem zakonu pripoznan tudi kot zavezanec po zakonodaji s področja obrambe, zasebnega varovanja in zaščite kritične infrastrukture lahko, skladno s podanimi usmeritvami pristojnega nacionalnega organa in predpisano metodologijo, že izdelano dokumentacijo navedenih področij dopolni z manjkajočimi zahtevami iz tega zakona.

(6) Zavezanci za namen obvladovanja incidentov, skladno z izvedeno analizo obvladovanja tveganj z oceno sprejemljivega nivoja tveganj, ki jo zavezanec izvede po predpisani metodologiji iz petega odstavka 6. člena tega zakona, zagotovijo tudi hrambo dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja, vendar ne manj kot šest mesecev. Hramba dnevniških zapisov mora biti zagotovljena na ozemlju RS.

(7) V kolikor obstaja področna zakonodaja posameznega sektorja ali sistema iz 5. člena tega zakona glede hrambe dnevniških zapisov, se upošteva področna zakonodaja.

(8) Ministrstvo, pristojno za informacijsko družbo, s pravilnikom podrobneje določi vsebino in strukturo varnostne dokumentacije, obseg in vsebino varnostnih ukrepov navedenih v 11. in 12. členu tega zakona ter metodologijo izvedbe analize obvladovanja tveganj.

13. člen

(ukrepi pristojnega nacionalnega organa)

(1) Ukrepi za preprečitev ponavljanja oziroma za zmanjšanje tveganja pojava incidenta so dejanja, ki so potrebna za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežja in informacijskih sistemov pred prepoznanimi grožnjami, ki jih zaznajo pristojni nacionalni organ, skupine CSIRT in zavezanci po tem zakonu. To so tudi dejanja, s katerimi zavezanec zmanjšuje vplive glede na nesprejemljivi nivo tveganja, ki jih je zavezanec prepoznal ob izvedeni analizi tveganja. Ukrepi se delijo na:
- splošna opozorila,
- odzivne ukrepe in
- zaščitne ukrepe.

(2) Splošna opozorila izda pristojni nacionalni organ z objavo na spletnih straneh in posredovanjem sporočila kontaktnim osebam iz prvega odstavka 7. člena tega zakona, kadar iz lastne zaznave ali

na pobudo nacionalnega ali vladnega CSIRT oziroma od pristojnih organov izve za kibernetske grožnje v informacijskem okolju, ki bi lahko ogrozile delovanje zavezancev.

(3) Kadar bi zaznane kibernetske grožnje v informacijskem okolju z večjo verjetnostjo lahko ogrozile nacionalno varnost, življenje in zdravje ljudi, javni red, ali bi grozila večja premoženjska škoda, mora pristojni nacionalni organ skupaj s pristojnimi organi o tem takoj obvestiti Sekretariat Sveta za nacionalno varnost. Vlada s sklepom določi posamezne naloge in njihove nosilce za učinkovito zmanjšanje zaznanega tveganja.

(4) Odzivne ukrepe za zmanjševanje učinkov incidenta na posameznem sektorju ali sistemu, ter za zmanjševanje medsektorskega vpliva na pobudo pristojnega nacionalnega organa določi inšpektor ali inšpektorica, pristojna za informacijsko varnost (v nadaljnjem besedilu: inšpektor). Inšpektor odzivne ukrepe določi s pisno odločbo, v časovni stiski pa tudi ustno in kasneje kakor hitro mogoče izda tudi pisno odločbo, ki jo izda zavezancu ali večjim zavezancem istega sektorja. Zavezanci o izvedbi prej navedenega ukrepa ter o njegovih rezultatih poročajo inšpektorju, skladno z roki, določenimi v odločbi.

(5) Zaščitne ukrepe na pobudo pristojnega nacionalnega organa določi inšpektor s pisno odločbo, v časovni stiski pa tudi ustno in kasneje kakor hitro mogoče izda tudi pisno odločbo, ki jo izda zavezancu ali večjim zavezancem istega sektorja z opozorilom, naj izvedejo analizo rešitve incidenta. Zavezanci o rezultatih analize poročajo inšpektorju skladno z rokom, določenim v odločbi.

(6) Kadar so predpisani odzivni in zaščitni ukrepi posledica zaznane kibernetske grožnje iz tretjega odstavka tega člena, so ukrepi označeni skladno s predpisano stopnjo tajnosti podatkov, kot jo opredeljuje zakon, ki ureja področje tajnih podatkov.

## VI. Standardizacija in prostovoljna priglasitev

14. člen

(standardizacija)

Za uskladitev pristopov izvajalcev bistvenih storitev in ponudnikov digitalnih storitev pri izvedbi ukrepov za obvladovanje tveganj za varnost omrežij in informacijskih sistemov ter za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost omrežij in informacijskih sistemov, ki se uporabljajo za zagotavljanje storitev, pristojni nacionalni organ spodbuja uporabo evropskih ali mednarodno sprejetih standardov in specifikacij s področja informacijske varnosti.

15. 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 ravnajo v skladu s postopkom iz 8. člena tega zakona.

(2) Skupine CSIRT pred prostovoljnimi priglasitvami prednostno obdelajo obvezne priglasitve.

Prostovoljne priglasitve se obdelajo le, kadar takšna obdelava skupinam CSIRT ne pomeni nesorazmernega ali neupravičenega bremena.

(3) Prostovoljna priglasitev subjektu priglasitelju ne sme naložiti nikakršnih obveznosti, ki zanj ne bi veljale, če ne bi opravil priglasitve.

## VII. Vrednotenje incidenta, stanje povišane ogroženosti in kibernetska obramba

16. člen

(vrednotenje incidenta)

(1) Lažji incident je enkraten incident z negativnim vplivom glede na zaupnost, celovitost in razpoložljivost omrežja ali informacijskega sistema zavezanca. Incident praviloma ne sme imeti večjega vpliva na nemoteno delovanje zavezanca, za kar se šteje izpad pod dve uri, ali povzročiti večje gospodarske škode zavezancu, ob tem da ne sme imeti medsektorskega vpliva ali vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti in sistema zaščite in reševanja.

(2) Težji incident je enkraten incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju z velikim negativnim vplivom glede na zaupnost, celovitost in razpoložljivost omrežja ali informacijskega sistema zavezanca. Incident ima večji vpliv na nemoteno delovanje zavezanca, za kar se šteje izpad nad dvema urama, ali povzroči večjo gospodarsko škodo zavezancu, ob tem ima lahko tudi medsektorski vpliv oziroma vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti in sistema zaščite in reševanja.

(3) Kibernetski napad je napad, ki povzroči oteženo delovanje države oziroma delno onemogoči delovanje vsaj treh sektorjev bistvenih storitev ali enega v celoti za več kot pet ur.

17. člen

(stanje povišane ogroženosti)

(1) Stanje povišane ogroženosti varnosti informacijskega okolja (v nadaljnjem besedilu: stanje povišane ogroženosti) pomeni stanje, ko je možnost realizacije zaznane kibernetske grožnje v informacijskem okolju izjemno velika.

(2) O stanju povišane ogroženosti pristojni nacionalni organ obvesti vlado in predlaga tudi ukrepe za zmanjšanje nastalega tveganja.

(3) V kolikor je potrebno tudi obveščanje širše javnosti, pristojni nacionalni organ skupaj z organom, pristojnim za komuniciranje z javnostjo, pripravi ustrezno sporočilo za javno objavo, ki so ga nacionalni mediji dolžni nespremenjenega objaviti.

(4) O posameznem stanju povišane ogroženosti lahko pristojni nacionalni organ po posvetu z vlado in organom, pristojnim za komuniciranje z javnostjo, posreduje splošno opozorilo po komunikacijskih kanalih, ki so dostopni javnosti.

18. člen

(kibernetska obramba)

(1) Kibernetsko obrambo izvajajo pristojni nacionalni organ, nacionalni in vladni CSIRT na podlagi tega zakona ter drugi pristojni organi skladno s svojimi pristojnostmi na podlagi njihove področne zakonodaje.

(2) Za namen kibernetske obrambe organi iz prejšnjega odstavka na različnih ravneh izvajajo organizacijske, logično-tehnične, tehnične ter netehnične ukrepe in aktivnosti.

## VIII. Seznami

19. člen

(vodenje in vsebina seznamov)

(1) Pristojni nacionalni organ za namen sodelovanja z zavezanci vodi seznam kontaktnih podatkov zavezancev, ki vsebuje:
- matične podatke poslovnega subjekta;
  - matično in davčno številko ter klasifikacijo dejavnosti subjekta,
  - naziv, naslov, telefonsko številko ter elektronski naslov subjekta,
  - ime in priimek zakonitega zastopnika subjekta,
- ime in priimek, naslov prebivališča, številko telefona in elektronski naslov kontaktne osebe za informacijsko varnost in njenega namestnika.

(2) Kopijo seznama kontaktnih podatkov zavezancev, za katere je pristojen, poseduje tudi posamezen CSIRT.

(3) Pristojni nacionalni organ za namen preprečevanja in odzivanja na incidente in kibernetske napade vodi skupni 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 ostalih pristojnih organov in postopek obveščanja morebitno prizadetih zavezancev,
- potek reševanja incidenta ali napada ter končni rezultat in sprejete ukrepe za preprečitev ponavljanja oziroma za zmanjšanje tveganja pojava incidenta ali napada.

(4) Skupine CSIRT za namen preprečevanja in odzivanja na incidente in kibernetske napade vodijo seznam incidentov in kibernetskih napadov s podatki kot v prejšnjem odstavku, za incidente, ki jih obdelujejo.

(5) Pristojni nacionalni organ in skupine CSIRT podatke, ki jih vsebujejo seznami iz tretjega in prejšnjega odstavka, na podlagi zakona, ki ureja tajne podatke, opredelijo kot tajne.

(6) Ne glede na prejšnji odstavek pristojni nacionalni organ in skupine CSIRT 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

20. člen

(strategija kibernetske varnosti)

(1) Strategija kibernetske varnosti predstavlja okvir za izvedbo ukrepov, ki bodo pripomogli k vzpostavitvi učinkovitega nacionalnega sistema zagotavljanja kibernetske varnosti. Opredeljuje ukrepe na naslednjih področjih:
- okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti;
- varnost državljanov v kibernetskem prostoru;
- kibernetska varnost v gospodarstvu;
- zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore;
- zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala;
- razvoj obrambnih kibernetskih zmogljivosti;
- zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah;
- krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem.

(2) V skladu s strategijo je nacionalni sistem za zagotavljanje informacijske varnosti zasnovan na dveh ravneh. Na strateški ravni deluje pristojni nacionalni organ, ki je hkrati tudi enotna kontaktna točka pri čezmejnem sodelovanju na tem področju. Pristojni nacionalni organ koordinira delo skupin CSIRT in ostalih zmogljivosti za zagotavljanje informacijske varnosti na operativni ravni sistema.

(3) Skrbnik nacionalne strategije kibernetske varnosti ter akcijskega načrta za njeno uresničevanje je pristojni nacionalni organ. Le-ta strategijo posodobi najmanj vsakih pet let.

21. člen

(pristojni nacionalni organ)

(1) Pristojni nacionalni organ ustanovi vlada.

(2) Pristojnosti na področju informacijske varnosti in kibernetske obrambe v RS izvaja pristojni nacionalni organ, če drug zakon ne določi drugače.

(3) Pristojni nacionalni organ:
1. koordinira delovanje sistema informacijske varnosti in kibernetske obrambe;
2. koordinira področje kriptologije;

3. izvaja obvladovanje incidentov v informacijskem okolju;
4. vodi sezname na podlagi tega zakona;
5. sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti in kibernetske obrambe, predvsem s skupinami CSIRT, ponudniki varnostnih rešitev in s sektorskimi varnostno operativnimi centri, če ti obstajajo, in z Agencijo za komunikacijska omrežja in storitve RS, informacijskim pooblaščencem ter z organi kazenskega pregona;
6. nudi strokovno podporo vsem zavezancem pri izvajanju njihovih nalog;
7. izvaja naloge mednarodnega sodelovanja na področju svojih pristojnosti;
8. zagotavlja analize, metodološko podporo in preventivno delovanje na področju informacijske varnosti ter daje mnenja s področja svojih prisotnosti;
9. je nacionalni koordinator usposabljanja, vaj in izobraževanja na področju informacijske varnosti ter skrbi za dvig zavedanja javnosti o informacijski varnosti;
10. spodbuja, koordinira in podpira raziskave in razvoj na področju informacijske varnosti;
11. je skrbnik nacionalne strategije kibernetske varnosti ter akcijskega načrta za njeno uresničevanje;
12. spremlja izvajanje tega zakona in podzakonskih predpisov, sprejetih na njegovi podlagi, po potrebi daje pobude za njihove spremembe in dopolnitve oziroma na poziv ministrstva, pristojnega za informacijsko družbo, pripravlja osnutke teh predpisov;
13. spremlja izvajanje NIS direktive v RS in Evropsko komisijo o tem redno obvešča. Pri tem ji posreduje predvsem informacije o ukrepih za določitev in številu ter pomenu izvajalcev bistvenih storitev, seznamu bistvenih storitev ter pragih za določitev ustrezne ravni opravljanja storitev;
14. je enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic ter z mrežo skupin CSIRT in s skupino za sodelovanje, v katero prispeva svojega predstavnika;
15. izpolnjuje obveznosti obveščanja in notifikacije Evropski komisiji in informacijske obveznosti do skupine za sodelovanje na podlagi ustreznega predpisa EU ter obveznosti obveščanja in notifikacije ostalih mednarodnih organizacij;
16. obvešča javnost o incidentih;
17. izvaja laboratorijsko dejavnost na področju informacijsko komunikacijske tehnologije;
18. razvija zmogljivosti za izvajanje kibernetske obrambe;
19. na podlagi varnostne dokumentacije zavezancev iz 11. člena tega zakona ter sektorskih načrtov nacionalnega in vladnega CSIRT in drugih pristojnih organov izdela nacionalni načrt odzivanja na incidente ali napade v informacijskem okolju in
20. izvršuje druge naloge na področju informacijske varnosti in kibernetske obrambe, določene s tem zakonom.

22.člen

(nacionalni CSIRT)

(1) Za zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov se na nacionalni ravni vzpostavi nacionalni CSIRT.

(2) Nacionalni CSIRT:
1. sprejema, obravnava, ocenjuje in se odziva na priglasitve incidentov s strani zavezancev, za katere je pristojen, ter te podatke evidentira, hrani in varuje;
2. zavezancem, za katere je pristojen nudi metodološko podporo, pomoč in sodelovanje ob pojavitvi incidenta;
3. na enak način v okviru zmožnosti sprejema priglasitve incidentov od organov in oseb, ki niso navedeni v 5. členu tega zakona in če to njegove kapacitete omogočajo, jih obdeluje in organom ali osebam, ki jih incident zadeva, nudi metodološko podporo, pomoč in sodelovanje;
4. vodi sezname na podlagi 19. člena tega zakona;
5. sprejema podatke o tveganjih in ranljivostih na področju informacijske varnosti, jih posreduje skrbnikom prizadetih sistemov in po potrebi objavlja opozorila;
6. sodeluje v mreži skupin CSIRT;
7. sodeluje s skupinami CSIRT v RS in v drugih državah;
8. izvaja nacionalni program ozaveščanja na področju informacijske varnosti, ki ga sprejme vlada.

(3) Nacionalni CSIRT mora imeti opravljeno akreditacijo pri evropskem združenju odzivnih centrov.

(4) Nacionalni CSIRT mora izpolnjevati zahteve za skupine za odzivanje na incidente na področju računalniške varnosti iz priloge 1 direktive NIS.

(5) Nacionalni CSIRT mora pri izpolnjevanju obveznosti na podlagi tretjega odstavka tega člena ravnati nepristransko.

23. člen

(vladni CSIRT)

(1) Za zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov se na vladni ravni vzpostavi vladni CSIRT.

(2) Vladni CSIRT:
1. sprejema, obravnava in ocenjuje priglasitve incidentov s strani zavezancev, za katere je pristojen, ter te podatke evidentira, hrani in varuje;
2. zavezancem, za katere je pristojen, nudi metodološko podporo, pomoč in sodelovanje ob pojavitvi incidenta;
3. vodi sezname na podlagi 19. člena tega zakona;

4. sodeluje v mreži skupin CSIRT;
5. sodeluje s skupinami CSIRT v RS in v drugih državah;
6. objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti.

(3) Vladni CSIRT mora izpolnjevati zahteve za skupine za odzivanje na incidente na področju računalniške varnosti iz priloge 1 direktive NIS.

24. člen

(sektorski varnostni operativni centri)

(1) Izvajalci bistvenih storitev iz posameznega sektorja, navedenega v drugem odstavku 5. člena tega zakona, lahko vzpostavijo sektorski varnostni operativni center (v nadaljnjem besedilu: SOC), če ocenijo, da je v posameznem sektorju to potrebno.

(2) Izvajalci bistvenih storitev iz prejšnjega odstavka o vzpostavitvi SOC obvestijo pristojni nacionalni organ, ki jim brezplačno nudi strokovno pomoč največ dve leti po tej seznanitvi.

(3) SOC pomaga zavezancem pri odzivanju na incidente.

25. člen

(sodelovanje na nacionalni ravni)

(1) Pristojni nacionalni organ, ki je hkrati tudi enotna kontaktna točka, ter nacionalni in vladni CSIRT sodelujejo pri izpolnjevanju obveznosti po tem zakonu. Pri tem nacionalni in vladni CSIRT svojo dejavnost usklajujeta s pristojnim nacionalnim organom.

(2) Nacionalni in vladni CSIRT pristojnemu nacionalnemu organu na varen način posredujeta tromesečna poročila na podlagi agregiranih priglasitev incidentov brez navedbe prijavitelja, istočasno pa imata tudi dostop do ažurnih kontaktnih informacij zavezancev, za katere sta pristojna.

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

## X. Inšpekcijski nadzor in odločanje o prekrških

26. člen

(pristojnost, postopek in pravna sredstva)

(1) Inšpektor izvaja inšpekcijski nadzor na področju informacijske varnosti. Pri izvrševanju inšpekcijskega nadzora inšpektor ugotavlja, ali zavezanci izpolnjujejo obveznosti, določene s tem zakonom in na njegovi podlagi sprejetimi podzakonskimi predpisi in akti ter ukrepi pristojnega

nacionalnega organa.

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

(3) Odločba inšpektorja, izdana v postopku inšpekcijskega nadzora na podlagi tega zakona, je v upravnem postopku dokončna, dovoljen pa je upravni spor.

(4) Tožba v upravnem sporu zoper dokončno odločbo, izdano na podlagi tega zakona, se vloži na sedežu Upravnega sodišča RS.

(5) Sodišče prve stopnje in sodišče, ki odloča o pravnih sredstvih, odločata o tožbah v upravnem sporu prednostno.

27. člen

(nadzor nad izvajalci bistvenih storitev)

(1) Inšpektor nadzira, ali izvajalci bistvenih storitev izpolnjujejo obveznosti iz 8. člena tega zakona ter s tem povezane posledice za varnost omrežij in informacijskih sistemov. Inšpektor lahko od zavezanca zahteva potrebne informacije in skupaj s pristojnim nacionalnim organom pripravi oceno varnosti omrežij in informacijskih sistemov ali pa od zavezanca pridobi oceno varnosti, ki jo je za njega pripravila organizacija, pooblaščena za izvedbo revizijskega pregleda informacijske varnosti oziroma kvalificiran revizor.

(2) Inšpektor lahko na osnovi ocene varnosti iz prejšnjega odstavka izvajalcem bistvenih storitev izreka ukrepe za odpravo ugotovljenih pomanjkljivosti.

(3) Pristojni nacionalni organ in pristojni CSIRT pri obravnavi incidentov, katerih posledica je kršitev varstva osebnih podatkov, sodelujeta z informacijskim pooblaščencem. Za namen pravočasnega ukrepanja v smeri zagotavljanja odprave kršitev pristojni nacionalni organ in pristojni CSIRT informacijskega pooblaščenca obveščata tudi v primerih suma kršitve varstva osebnih podatkov.

28. člen

(nadzor na ponudniki digitalnih storitev)

(1) Inšpektor lahko ukrepa, če so mu predloženi dokazi, da ponudnik digitalnih storitev ne izpolnjuje zahtev iz 9. člena tega zakona. Takšne dokaze lahko predloži tudi pristojen organ druge države članice EU, v kateri se storitev zagotavlja.

(2) Inšpektor lahko od ponudnikov digitalnih storitev zahteva informacije, potrebne za oceno varnosti njihovega omrežja in informacijskih sistemov ter za oblikovanje ukrepov zaradi neizpolnjevanja zahtev iz 9. člena tega zakona.

29. člen

(inšpekcijski ukrepi)

(1) Če inšpektor pri nadzoru ugotovi pomanjkljivosti, nadzorovanemu zavezancu določi način in rok za

njihovo odpravo.

(2) Če omrežju in informacijskemu sistemu zavezanca zaradi ugotovljenih pomanjkljivosti grozi incident ali napad, ki ga lahko znatno poškoduje ali uniči, lahko inšpektor zavezancu v skrajnem primeru prepove uporabo tega sistema ali njegovega dela, dokler ni ugotovljena pomanjkljivost odpravljena.

30. člen

(prekrškovni postopek)

(1) Inšpektor odloča o prekrških za kršitve tega zakona in na njegovi podlagi izdanih predpisov kot prekrškovni organ v skladu z zakonom, ki ureja prekrške.

(2) Prekrškovni postopki se rešujejo po hitrem postopku v skladu z zakonom, ki ureja prekrške.

(3) Prekrškovni organ lahko za prekrške iz tega zakona izreče globo v znesku, višjem od najnižje predpisane mere za posamezni prekršek.

## XI. Kazenske določbe

31. člen

(prekrški)

(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 ali drugega odstavka 7. člena tega zakona,
- ne izpolni obveznosti iz prvega, drugega, tretjega ali četrtega odstavka 8. člena tega zakona,
- ne obvesti pristojnih organov kazenskega pregona skladno s petim odstavkom 8. člena tega zakona,
- ob prijavi incidenta ne poskrbi za ustrezno zavarovanje podatkov revizijskih sledi skladno s šestim odstavkom 8. člena tega zakona,
- ne izpolni obveznosti glede varnostne dokumentacije iz 11. člena tega zakona,
- ne izpolni obveznosti glede hrambe dnevniških zapisov iz šestega odstavka 12. 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, ki stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 200 do 2.000 eurov se kaznuje odgovorna oseba v državnem organu, samoupravni lokalni skupnosti ali v drugi osebi javnega prava, ki je zavezanec po tem zakonu, če stori prekršek iz prvega odstavka tega člena.

## XII. Prehodne določbe

32. člen

(ustanovitev in pričetek delovanja pristojnega nacionalnega organa)

(1) Pristojni nacionalni organ iz prvega odstavka 21. člena tega zakona ustanovi vlada najkasneje v treh mesecih po uveljavitvi tega zakona.

(2) Pristojni nacionalni organ iz prejšnjega odstavka prične z delovanjem po tem zakonu dne 1. 1. 2019.

(3) Z dnem začetka njegovega delovanja, pristojni nacionalni organ od UVTP prevzame naloge, arhive in dokumentacijo, ki se nanaša na kibernetsko varnost.

(4) Vlada na predlog ministrstva, pristojnega za varstvo tajnih podatkov, v roku treh mesecev od uveljavitve tega zakona uskladi Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uradni list RS, št. 6/02 in 17/17) z določbami tega zakona.

33. člen

(delovanje drugih pristojnih organov)

(1) Vlada določi izvajalca nalog nacionalnega CSIRT, ki jih ta začne izvajati skladno s tem zakonom dne 1. 1. 2019. Do 1. 1. 2019 izvaja naloge nacionalnega CSIRT odzivni center SI-CERT pri Akademski in raziskovalni mreži Slovenije.

(2) Vladni CSIRT mora biti v skladu z zahtevami tega zakona vzpostavljen na ministrstvu, pristojnem za upravljanje informacijsko komunikacijskih sistemov državne uprave najkasneje v roku šestih mesecev od dneva uveljavitve tega zakona. Do vzpostavitve vladnega CSIRT se njegove naloge izvajajo kot naloge nacionalnega CSIRT skladno s prejšnjim odstavkom.

34. člen

(izdaja podzakonskih predpisov)

(1) Rok za izdajo podzakonskih predpisov, ki so po tem zakonu obvezni, je največ šest mesecev od dneva uveljavitve tega zakona.

(2) Vlada uskladi uredbo, ki ureja organe v sestavi ministrstev z določbami tega zakona najkasneje v roku treh mesecev po uveljavitvi tega zakona.

35. člen

(prehodno obdobje)

(1) Vlada s sklepom določi izvajalce bistvenih storitev iz 5. člena tega zakona v roku treh mesecev od uveljavitve uredbe iz petega odstavka 6. člena tega zakona.

(2) Pristojni nacionalni organ v roku 30 dni od uveljavitve sklepa iz prejšnjega odstavka vpiše izvajalce

bistvenih storitev v seznam iz šestega odstavka 5. člena tega zakona in o njihovem statusu pisno obvesti zavezance skladno sedmim odstavkom 5. člena tega zakona.

(3) Izvajalci bistvenih storitev morajo izpolniti varnostne zahteve in zahteve za priglasitev incidentov najkasneje v šestih mesecih od prejema odločbe o statusu zavezanca.

## XIII. Končna določba

36. člen

(začetek veljavnosti)

Ta zakon prične veljati petnajsti dan po objavi v Uradnem listu RS.