REPUBLIKA SLOVENIJA
VLADA REPUBLIKE SLOVENIJE

Gregorčičeva 20–25, SI-1001 Ljubljana

T: +386 1 478 1000
F: +386 1 478 1607
E: gp.gs@gov.si
http://www.vlada.si/

PREDLOG
EVA: 2017-3130-0029
PRVA OBRAVNAVA

ZAKON
O INFORMACIJSKI VARNOSTI

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

V Republiki Sloveniji (v nadaljnjem besedilu: RS) je bilo v preteklosti že pripravljenih nekaj predlogov sistemske ureditve področja informacijske varnosti, vendar do izvedbe nikoli ni prišlo. Korak naprej je bil storjen leta 2016, ko je Vlada sprejela Strategijo kibernetske varnosti, ki je podlaga za pripravo in izvedbo ukrepov na področju zagotavljanja informacijske varnosti.

Vlada RS je 6. aprila 2017 sprejela Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov (v nadaljnjem besedilu: UVTP) (Uradni list RS, št. 17/17). S tem sklepom so bile določene strokovne naloge in organizacija UVTP na področju kibernetske varnosti. UVTP je tako postal tudi pristojni organ na strateški ravni nacionalnega sistema informacijske varnosti.

Na operativni ravni sistema so zmogljivosti za odzivanje na incidente v kibernetskem prostoru porazdeljene med SI-CERT kot nacionalni odzivni center za omrežne incidente, Sektor za informacijsko varnost v okviru Direktorata za informatiko na Ministrstvu za javno upravo (v nadaljnjem besedilu: MJU), Ministrstvo za obrambo (v nadaljnjem besedilu: MO) za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Slovensko obveščevalno-varnostno agencijo (v nadaljnjem besedilu: SOVA) na področju protiobveščevalnega delovanja ter Policijo, Urad za informatiko in telekomunikacije in Upravo kriminalistične policije, predvsem Center za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala. Organi na obeh ravneh sistema so podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju.

RS do zdaj ni imela zakonsko urejenega področja zagotavljanja informacijske varnosti. Naraščajoči trend obsega incidentov v kibernetskem prostoru in velika odvisnost gospodarstva ter celotne družbe od neprekinjenega delovanja omrežij in informacijskih sistemov pa zahtevajo celovito ureditev in tudi okrepitev področja zagotavljanja informacijske varnosti. Državo k temu spodbujajo in jo hkrati zavezujejo tudi sprejeti strateški domači in mednarodni dokumenti, na primer Resolucija o strategiji nacionalne varnosti RS, Strategija kibernetske varnosti Evropske unije (v nadaljnjem besedilu: EU) »Odprt, varen in zavarovan kibernetski prostor« in sprejeti nacionalna Strategija kibernetske varnosti ter 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 (v

nadaljnjem besedilu: Direktiva 2016/1148/ES), ki mora biti v nacionalne pravne rede držav članic prenesena do 9. maja 2018.

Ob tem je treba pojasniti, da za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve (v nadaljnjem besedilu: operaterji), veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev iz VII. poglavja (Varnost omrežij in storitev ter delovanje v izjemnih stanjih) Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17; v nadaljnjem besedilu: ZEKom-1), kjer gre za prenos 13.a in 13.b člena Direktive 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (Okvirna direktiva). Operaterji morajo namreč sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev, zlasti zaradi preprečevanja in zmanjševanja učinkov varnostnih incidentov na uporabnike in medsebojno povezana omrežja. Sprejeti ukrepi morajo ob upoštevanju stanja zagotoviti raven varnosti, primerno predvidenemu tveganju. Določene so tudi obveznosti obveščanja in poročanja o kršitvah varnosti ali celovitosti Agenciji za komunikacijska omrežja in storitve RS (v nadaljnjem besedilu: AKOS), ki potem po potrebi poroča UVTP. Iz tega razloga Direktiva 2016/1148/ES v tretjem odstavku 1. člena operaterje izključuje iz svojega dometa, temu pa sledi tudi predlog ZIV.

Določbe ZIV se ne bodo uporabljale tudi za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 (tako imenovana Uredba eIDAS), ki jih Direktiva 2016/1148/ES v tretjem odstavku 1. člena prav tako izključuje.

Direktiva 2016/1148/ES

Direktiva 2016/1148/ES, sprejeta 6. julija 2016, želi zagotoviti krepitev obrambnih kibernetskih zmogljivosti na nacionalnih ravneh držav članic, krepitev kibernetske varnosti EU z mednarodnim sodelovanjem in uvedbo obveznega upravljanja s tveganji in poročanja o incidentih za izvajalce bistvenih storitev in ponudnike digitalnih storitev.

Vsaka država članica mora sprejeti nacionalno strategijo za varnost omrežij in informacijskih sistemov ter ustrezno določiti strateške cilje in regulativne ukrepe. Ključne točke strategije so strateški cilji, prednostne naloge in model upravljanja, merila za ustrezno stopnjo pripravljenosti, odzivnosti in zmogljivosti za ponovno vzpostavitev stanja po incidentu, sodelovanje javnega in zasebnega sektorja, izvajanje programov ozaveščanja in uvedba vsebin s področja kibernetske varnosti za izobraževanje in usposabljanje, okvirni program za raziskave in razvoj na področju kibernetske/informacijske varnost, okvirni program za oceno in upravljanje s tveganji ter seznam ključnih akterjev za izvajanje strategije.

Države članice morajo določiti enega ali več pristojnih nacionalnih organov za varnost omrežij in informacijskih sistemov, ki spremljajo uporabo Direktive NIS na nacionalni ravni. Poleg tega morajo določiti enotno kontaktno točko za komunikacijo in sodelovanje z relevantnimi organi v drugih državah članicah ter enega ali več nacionalnih odzivnih centrov CSIRT (angl. Computer security incident response team), ki so odgovorni za nadzor in spremljanje incidentov na nacionalni ravni, zagotavljanje zgodnjega odkrivanja, vzpostavitev učinkovitega sistema obveščanja ter razširjanje informacij o tveganjih in incidentih med ključnimi skupinami, odziv na incidente, oceno tveganj in možnosti incidentov ter stopnje ozaveščenosti o kibernetski izpostavljenosti in sodelovanje v mreži nacionalnih odzivnih centrov CSIRT. Mrežo CSIRT sestavljajo predstavniki držav članic, centrov

CSIRT in CERT-EU. Evropska komisija (v nadaljnjem besedilu: EK) sodeluje v mreži CSIRT kot opazovalka. Agencija EU za varnost omrežij in informacije (v nadaljnjem besedilu: ENISA) sodeluje v vlogi sekretariata in podpore sodelovanju med odzivnimi centri CSIRT. Države članice ob tem zagotovijo, da imajo pristojni nacionalni organi, enotna kontaktna točka in nacionalni odzivni centri CSIRT ustrezne vire za učinkovito izvajanje nalog, za katere so skladno z Direktivo NIS pristojni. Pri tem države članice zaradi izvajanja in izvrševanja Direktiva 2016/1148/ES tudi zagotovijo, da imajo pristojni organi potrebna pooblastila in sredstva za izvajanje nadzornih pooblastil oziroma pristojnosti.

Direktiva 2016/1148/ES določa oblikovanje skupine za sodelovanje za podporo sodelovanju na strateški ravni, izmenjavo informacij med državami članicami in vzpostavitev medsebojnega zaupanja. Direktiva določa tudi vzpostavitev mreže CSIRT za zagotavljanje pogojev medsebojnega zaupanja med državami članicami in za spodbujanje hitre komunikacije ter učinkovitega sodelovanja na operativni ravni. Mreža CSIRT med drugim izmenjuje informacije o kapacitetah odzivnih centrov, dejavnostih in možnostih sodelovanja, informacije o incidentih (na zahtevo in na prostovoljni podlagi), prepoznava situacije, ki zahtevajo koordiniran odziv na incidente (na zahtevo in na prostovoljni podlagi), izvaja podporo pri čezmejnemu obravnavanju incidentov (na prostovoljni podlagi), išče nove oblike sodelovanja na operativni ravni, obvešča skupino za sodelovanje o aktivnostih in zahtevkih za smernice o nadaljnjih postopkih, ponuja možnost razprave o znanju in izkušnjah, pridobljenih v okviru usposabljanj, in objavlja smernice za sodelovanje na operativni ravni.

Vsaka država članica mora določiti svoje izvajalce bistvenih storitev. Osnovna merila za določitev so, da je subjekt izvajalec storitev, ki so ključnega pomena za vzdrževanje in nemoteno delovanje gospodarskih in družbenih dejavnosti, da je nemoteno delovanje storitev izvajalca odvisno od delovanja omrežja in informacijskih sistemov ter da bi varnostni incident prekinil ali resno okrnil delovanje storitev, ki jih izvajalec zagotavlja. Pri določanju stopnje resnosti incidenta naj bi upoštevali, kakšno je število prizadetih uporabnikov, trajanje incidenta in geografsko razširjenost oziroma doseg incidenta. Direktiva zajema naslednja področja:

- energija,
- digitalna infrastruktura,
- oskrba s pitno vodo in njena distribucija,
- zdravstvo,
- promet,
- bančništvo,
- infrastruktura finančnega trga.

Varnost, neprekinjenost in zanesljivost vrste digitalnih storitev iz Direktive NIS so ključne za nemoteno delovanje številnih podjetij. Prekinitev take digitalne storitve bi lahko preprečila zagotavljanje drugih storitev, ki so od nje odvisne, in bi tako lahko vplivala na ključne ekonomske in družbene dejavnosti v EU. Take digitalne storitve bi tako lahko bile ključnega pomena za nemoteno delovanje podjetij, ki so od njih odvisna, ter zlasti za udeležbo teh podjetij na notranjem trgu in čezmejno trgovino v EU. Ta direktiva se uporablja za tiste ponudnike digitalnih storitev, za katere se šteje, da ponujajo digitalne storitve, od katerih so številna podjetja v EU vse bolj odvisna.

Stopnja tveganja za izvajalce bistvenih storitev, ki so pogosto bistvene za ohranjanje ključnih družbenih in gospodarskih dejavnosti, je v praksi višja od stopnje tveganja za ponudnike digitalnih

storitev. Zato direktiva navaja, da bi morale biti varnostne zahteve za ponudnike digitalnih storitev manj stroge. Ponudnikom digitalnih storitev bi morali omogočiti, da se sami odločijo za sprejetje ukrepov, ki se jim zdijo primerni za obvladovanje tveganj, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov. Zaradi čezmejne narave ponudnikov digitalnih storitev bi se moral zanje uporabljati bolj usklajen pristop na ravni EU. Z izvedbenimi akti bi morali zagotoviti lažjo določitev in izvajanje tovrstnih ukrepov. V tem smislu Direktiva 2016/1148/ES določa ponudnike digitalnih storitev, in sicer so to spletne tržnice, storitve računalništva v oblaku ter iskalniki. Za vse subjekte, ki ustrezajo tej opredelitvi, samodejno veljajo varnostne zahteve in obveznost priglasitve v skladu z Direktivo 2016/1148/ES. To pa ne velja za mikro in mala podjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro-, malih in srednjih podjetij (UL L 124, 20. 5. 2003, str. 36) in se nanj sklicuje Direktiva 2016/1148/ES.

Za usklajen, a prožen pristop za ponudnike digitalnih storitev bo EK sprejela izvedbene akte o varnostnih zahtevah in obveznosti priglasitve. Države članice zanje ne morejo dodatno zaostriti zahtev po varnosti in obveznosti priglasitve. Poleg tega bodo pristojni organi lahko opravljali nadzor le v primeru dokaza, da ponudnik digitalnih storitev ni izpolnjeval svojih obveznosti, kot so določene v Direktivi 2016/1148/ES.

Direktiva 2016/1148/ES se torej uporablja tako za izvajalce bistvenih storitev kot tudi za ponudnike digitalnih storitev. Vendar se obveznosti izvajalcev bistvenih storitev in ponudnikov digitalnih storitev ne uporabljajo za podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve v smislu Okvirne direktive, za katera veljajo posebne zahteve glede varnosti in celovitosti, določene v navedeni direktivi. Prav tako se ne uporabljajo za ponudnike storitev zaupanja v smislu Uredbe eIDAS, za katere veljajo varnostne zahteve iz navedene uredbe, kot je bilo navedeno zgoraj.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji

Republika Slovenija bo z Zakonom o informacijski varnosti (v nadaljnjem besedilu tudi: ZIV) v svoj pravni red prenesla Direktivo 2016/1148/ES, katere cilj in namen je zagotoviti visoko skupno raven varnosti omrežij in informacijskih sistemov v EU. Poleg tega bo z zakonom sistemsko uredila področje informacijske varnosti tako na strateški kot tudi na operativni ravni nacionalnega sistema zagotavljanja informacijske varnosti, razen na področjih, ki sta izključeni, in sicer se predlog zakona ne uporablja za operaterje, za katere veljajo posebne obveznosti glede varnosti in celovitosti omrežij in ZEKom-1, ter za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe eIDAS.

2.2 Načela

Predlog zakona, podobno kot Direktiva 2016/1148/ES, upošteva spoštovanje človekovih pravic in temeljnih svoboščin, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo gospodarske pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča ter pravico podati izjavo. Ob tem predlog zakona upošteva tudi načelo ekonomičnosti (v smislu preprečevanja podvajanja administrativnih bremen) ter načela pravne države, in sicer pravne varnosti in sorazmernosti.

2.3 Poglavitne rešitve

– Predstavitev predlaganih rešitev

V nadaljevanju so po poglavjih predstavljene poglavitne rešitve predloga zakona.

I. Splošne določbe

- vsebina predloga zakona ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v RS, zavezancem določa minimalne zahteve glede varnosti in priglasitve incidentov ter določa pristojnosti, naloge, organizacijo in delovanje novega pristojnega nacionalnega organa (PNO), enotne kontaktne točke za varnost omrežij in informacijskih sistemov (enotna kontaktna točka), nacionalne skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (nacionalni CSIRT) ter skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (CSIRT organov državne uprave);
- namen predloga zakona je ureditev področja informacijske varnosti in 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, in prenos Direktive 2016/1148/ES. Iz področja uporabe predloga zakona so izključeni operaterji, za katere že veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev iz zakona, ki ureja elektronske komunikacije, ter ponudniki storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014, ker ti izjemi izhajata iz Direktive 2016/1148/ES;
- pomen izrazov je skladen z Direktiva 2016/1148/ES, ko gre za nacionalne določbe, pa s strokovnimi pojmi s področja informacijske varnosti oziroma obramboslovja;
- pri obdelavi podatkov na podlagi tega zakona se ta glede osebnih podatkov izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, če pa so podatki in informacije, ki se obdelujejo, opredeljeni kot tajni ali kot poslovna skrivnost, pa v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost.

II. Zavezanci

- zavezanci so izvajalci bistvenih storitev (IBS), ponudniki digitalnih storitev (PDS) ter 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);
- IBS so subjekti (javni ali zasebni), ki delujejo na naslednjih področjih: energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo in infrastruktura finančnega trga, preskrba s hrano in varstvo okolja;
- IBS bo določila vlada na podlagi zakonskih meril po tem, ko bo (z uredbo) določila tiste storitve na posameznih področjih, ki se štejejo za bistvene in določila metodologijo za določitev IBS ter področne dejavnike, ki vplivajo na oceno negativnega vpliva incidentov. IBS so tudi tisti upravljavci kritične infrastrukture, določeni v skladu s predpisi, ki urejajo področje kritične infrastrukture, in nosilci obrambnega načrtovanja, določeni v skladu s predpisi, ki urejajo področje obrambe, katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov (tudi te IBS določi vlada);
- PDS so zavezani neposredno na podlagi zakona, izključena pa so tisti, ki glede na število zaposlenih in letni promet oziroma letno bilančno vsoto ne presegajo kriterijev za majhna (s

tem vključno tudi mikro) podjetja, skladno z opredeljenimi merili na katere se sklicuje Direktiva 2016/1148/ES, ki zahteva visoko stopnjo harmonizacije za PDS (digitalne storitve so ob tem storitve informacijske družbe, spletne tržnice, spletnega iskalnika in računalništva v oblaku);

- vlada določi tudi zavezane organe državne uprave;
- IBS določijo kontaktne osebe za informacijsko varnost ter kontaktne podatke teh oseb v določenih rokih posredujejo pristojnemu nacionalnemu organu, za PDS (glede na visoko stopnjo harmonizacije na ravni EU) pa to ni zahteva, temveč le možnost, ob upoštevanju centralizacije državne informatike je to tudi le možnost za organe državne uprave.

III. Informacijska varnost izvajalcev bistvenih storitev

- določene so ključne varnostne zahteve za IBS, vključno z predvideno varnostno dokumentacijo, na podlagi katere morajo IBS pripraviti in izvajati potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe, vsebino pa bo podrobneje uredil pristojni minister (s pravilnikom). IBS zaradi obvladovanja incidentov zagotovijo ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja (ne manj kot šest mesecev) v RS, razen za področje digitalna infrastruktura, bančništvo in infrastruktura finančnega trga, pri katerih se to lahko zagotavlja na ozemlju EU;
- z namenom zmanjševanja administrativnih bremen, zagotavljanja pravne varnosti in sorazmernosti lahko IBS v primeru, da že imajo izdelano varnostno dokumentacijo na podlagi drugih predpisov, to (le) dopolnijo skladno s tem zakonom;
- IBS nacionalnemu CSIRT priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev, ki jih zagotavljajo, in podajo informacije, na podlagi katerih se določi pomembnost morebitnega čezmejnega vpliva. Predpisani so kriteriji za določitev pomembnosti vpliva priglašenega incidenta, IBS pa morajo ob priglasitvi poskrbeti za zavarovanje dnevniških zapisov oziroma revizijskih sledi, če te obstajajo;
- določene so pristojnosti nacionalnega CSIRT, pristojnega nacionalnega organa in drugih pristojnih organov, ki morajo biti v določenih primerih z incidentom seznanjeni, kot tudi obveščanje in izmenjava informacij znotraj EU ter obveščanje javnosti, vse v primerih in na način, kot je potrebno in sorazmerno.

IV. Informacijska varnost ponudnikov digitalnih storitev

- PDS določijo ter sprejmejo ustrezne in sorazmerne tehnične ter organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju teh storitev. S temi ukrepi PDS zagotovijo raven varnosti omrežij in informacijskih sistemov, ki je primerna tveganju, ter za ta namen upoštevajo v zakonu navedene elemente, PDS sprejmejo tudi ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki jih ogrožajo, da bi zagotovili neprekinjeno izvajanje svojih storitev;
- PDS nacionalnemu CSIRT priglasijo vsak incident, ki ima pomemben vpliv na zagotavljanje digitalnih storitev. Priglasitev zajema informacije, na podlagi katerih se določi pomembnost morebitnega čezmejnega vpliva. Obveznost priglasitve incidenta za PDS velja le, kadar ima ta dostop do informacij, potrebnih za oceno vpliva incidenta. Zato je (skladno z Direktivo 2016/1148/ES) dodatno zavezan IBS, če je pri opravljanju svojih storitev odvisen od PDS, da priglasi vsak znaten vpliv na neprekinjeno izvajanje bistvenih storitev, ki je posledica incidenta, ki vpliva na PDS;

- določene so pristojnosti nacionalnega CSIRT in pristojnega nacionalnega organa, kot tudi obveščanje in izmenjava informacij znotraj EU ter obveščanje javnosti, vse v primerih in na način, kot je potrebno in sorazmerno;
- določena so pravila pristojnosti za PDS, pri čemer so organi v RS pristojni (skladno z Direktivo 2016/1148/ES), če ima PDS glavni sedež v RS (glavni sedež je tam, kjer je glavna uprava) ali če ima PDS v RS sedež svojega predstavnika. PDS, ki nima sedeža v EU, v njej pa zagotavlja takšne storitve, mora namreč v EU določiti sedež svojega predstavnika, ki zastopa PDS v zvezi z njihovimi obveznostmi. Tudi če organi RS niso pristojni za PDS, pristojni organi RS sodelujejo in si medsebojno pomagajo s pristojnimi organi drugih držav članic EU ter si po potrebi izmenjujejo informacije na način, kot je potrebno in sorazmerno.

V. Informacijska varnost organov državne uprave

- predlog zakona za organe državne uprave določa ključne varnostne zahteve, vključno z v zakonu predvideno varnostno dokumentacijo, na podlagi katere le-ti pripravijo in izvajajo potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe, vsebino pa bo podrobneje uredil pristojni minister (s pravilnikom). Organi državne uprave z namenom obvladovanja incidentov zagotovijo ohranjanje dnevniških zapisov o delovanju svojih informacijskih sistemov ali delov omrežja (ne manj kot šest mesecev) na ozemlju RS;
- z namenom zmanjševanja administrativnih bremen, zagotavljanja pravne varnosti in sorazmernosti lahko organi državne uprave v primeru, da že imajo izdelano varnostno dokumentacijo na podlagi drugih predpisov, to (le) dopolnijo skladno s tem zakonom;
- organi državne uprave priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje njihovih storitev na CSIRT organov državne uprave, tisti organi državne uprave, ki imajo lastne zmogljivosti vsaj na ravni SOC, pa pristojnemu nacionalnemu organu , pri čemer so predpisani kriteriji za določitev pomembnosti vpliva incidenta, organi državne uprave pa poskrbijo za zavarovanje dnevniških zapisov oziroma revizijskih sledi, če te obstajajo;
- predlog zakona ob priglasitvi, ki jo izvedejo organi državne uprave, ureja pristojnosti in medsebojno sodelovanje CSIRT organov državne uprave, nacionalnega CSIRT, pristojnega nacionalnega organa in drugih pristojnih organov ter obveščanje javnosti, vse v primerih in na način, kot je potrebno in sorazmerno.

VI. Standardizacija in prostovoljna priglasitev

- zaradi uskladitve pristopov IBS, PDS in organov državne uprave pri izvajanju njihovih obveznosti pristojni nacionalni organ spodbuja uporabo standardov in specifikacij, in v ta namen ustrezne informacije objavlja na svojih spletnih straneh;
- subjekti, ki niso zavezanci, lahko prostovoljno priglašajo incidente, ki imajo pomemben vpliv na neprekinjeno izvajanje njihovih storitev. Pravila obdelave prostovoljnih priglasitev so zakonsko predvidena, pri čemer nacionalni CSIRT in CSIRT organov državne uprave v vsakem primeru prednostno obdelata obvezne priglasitve.

VII. Vrednotenje incidenta, stanje povečane ogroženosti in kibernetska obramba

- priglašene incidente glede na predvidene kriterije vrednotita nacionalni CSIRT ali CSIRT organov državne uprave, po potrebi v sodelovanju s pristojnim nacionalnim organom, pri čemer lahko gre za lažji, težji ali kritični incident. Pristojni nacionalni organ na podlagi podatkov in informacij o teži incidenta oceni, ali gre hkrati za kibernetski napad, pri tem

zavezancem v primeru težjega ali kritičnega incidenta ali v primeru kibernetskega napada z odločbo lahko določi takšne ustrezne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic, ti ukrepi pa morajo biti določeni v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena;

- 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 (pomeni stanje, ko je podana velika verjetnost realizacije težjega ali kritičnega incidenta oziroma kibernetskega napada v 72 urah od zaznave takšne verjetnosti), ter lahko v teh primerih za IBS in organe državne uprave z odločbo določi takšne ustrezne in sorazmerne ukrepe, kot je potrebno za preprečitev ali za zmanjšanje verjetnosti realizacije incidenta ali pričakovanih škodljivih posledic ob morebitni realizaciji takšnega incidenta. Pri tem se ukrepi določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena;
- pristojni nacionalni organ obvešča vlado in Svet za nacionalno varnost (SNAV) o kritičnem incidentu in kibernetskem napadu ter o stanju povečane ogroženosti zaradi verjetnosti realizacije kritičnega incidenta ali kibernetskega napada, lahko pa ju obvešča tudi o težjih incidentih ali verjetnosti realizacije takšnega incidenta. Obveščanje vlade in SNAV je obvezno tudi v vseh primerih, kadar je bila v zvezi z incidentom ali njegovim pričakovanjem izdana odločba z ukrepi. V zvezi s sprejetimi ukrepi sta urejena tudi postopek in način obveščanja širše javnost, kar je naloga pristojnega nacionalnega organa (splošno opozorilo), če je takšno obveščanje glede na okoliščine potrebno;
- kibernetsko obrambo (celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade) usklajujejo in izvajajo pristojni nacionalni organ, nacionalni CSIRT in CSIRT organov državne uprave ter ministrstvo, pristojno za obrambo, policija, Slovenska obveščevalno-varnostna agencija (SOVA) in drugi nacionalni organi skladno s svojimi pristojnostmi pri zagotavljanju nacionalne varnosti, ki za ta namen lahko na različnih ravneh izvajajo usklajene organizacijske, logično-tehnične, tehnične in administrativne ukrepe in dejavnosti za zagotavljanje celovite informacijske varnosti.

VIII. Seznami

- predlog zakona ureja vodenje in vsebino seznamov, pri čemer pristojni nacionalni organ za namen sodelovanja z zavezanci vodi seznam kontaktnih podatkov, do katerega imata v delu, ki se nanaša na zavezance iz njune pristojnosti, dostop tudi nacionalni CSIRT in CSIRT organov državne uprave. Pristojni nacionalni organ za namen preprečevanja incidentov in kibernetskih napadov ter odzivanja na njih vodi skupni seznam incidentov in kibernetskih napadov, nacionalni CSIRT in CSIRT organov državne uprave pa za enak namen vodita seznam tistih incidentov in kibernetskih napadov, ki jih obravnavata. Pristojni nacionalni organ za namen določitve IBS vodi seznam bistvenih storitev, za namen določitve organov državne uprave pa seznam informacijskih sistemov, storitev in delov omrežja, nujnih za nemoteno delovanje države ali zagotavljanje nacionalne varnosti;
- pristojni organi, ki vodijo sezname 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

- strategija informacijske varnosti (strategija) je osnovni okvir za izvedbo ukrepov, ki bodo pripomogli k vzpostavitvi učinkovitega nacionalnega sistema zagotavljanja informacijske varnosti;
- pristojni nacionalni organ je organ v sestavi ministrstva, pristojnega za informacijsko družbo (predvidoma tako imenovana »Uprava RS za informacijsko varnost«). Pristojni nacionalni organ poleg drugih nalog, določenih s predlogom tega zakona, izvaja še naloge, ki so taksativno naštete v določbi o pristojnem nacionalnem organu. Pri tem na primer koordinira delovanje sistema informacijske varnosti, razvija zmogljivosti za izvajanje kibernetske obrambe, zavezancem nudi strokovno podporo, sodeluje z drugimi pristojnimi organi in organizacijami, je enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in izvaja druge naloge mednarodnega sodelovanja;
- za nacionalni CSIRT je določen odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri javnem zavodu Akademska in raziskovalna mreža Slovenije, ki poleg drugih nalog, določenih s predlogom tega zakona, izvaja še naloge, ki so taksativno naštete v določbi o nacionalnem CSIRT;
- naloge CSIRT organov državne uprave izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave, ki poleg drugih nalog, določenih s predlogom tega zakona, izvaja še naloge, ki so taksativno naštete v določbi o CSIRT organov državne uprave;
- predlog zakona določa, da IBS v sodelovanju in s soglasjem pristojnih organov s področja njihovega delovanja, lahko vzpostavijo še področni SOC, če ocenijo, da je na posameznem področju to potrebno, pri čemer morajo o tem obvestiti pristojni nacionalni organ ter nacionalni CSIRT, področni SOC pa sodeluje z obema ter pomaga IBS pri odzivanju na incidente, področni SOC lahko na svojem področju dela vzpostavijo tudi organi državne uprave;
- pristojni nacionalni organ ter nacionalni CSIRT in CSIRT organov državne uprave sodelujejo pri izpolnjevanju obveznosti po tem zakonu. Pri tem nacionalni CSIRT in CSIRT organov državne uprave svojo dejavnost usklajujeta s pristojnim nacionalnim organom in mu štirikrat letno na varen način posredujeta poročilo o izvajanju svojih pristojnosti na podlagi tega zakona.

X. Nadzor

- predlog zakona predvideva, da bodo nadzor nad izvajanjem njegovih določb, na njegovi podlagi sprejetih predpisov in nad izvajanjem upravnih odločb, izdanih na njegovi podlagi, opravljali inšpektorji za informacijsko varnost v okviru pristojnega nacionalnega organa;
- inšpektor lahko poleg ukrepov, ki jih ima po zakonu, ki ureja inšpekcijski nadzor, odredi še ukrepe, določene s tem zakonom, pri čemer mora inšpektor, če gre hkrati za kršitev varstva osebnih podatkov ali če sumi, da gre za to, obveščati in sodelovati z Informacijskim pooblaščencem. Navedeno je za IBS in PDS posledica zahtev Direktive 2016/1148/ES, skladno pa se ureja tudi za organe državne uprave;
- ne glede na določbe zakona, ki ureja inšpekcijski nadzor, lahko inšpektor zavezancem le v skrajnem primeru in upoštevaje področni pomen sistema ter njihovo dejavnost prepove uporabo tega sistema ali njegovega dela, dokler ni ugotovljena pomanjkljivost odpravljena in če s tem ukrepom ni ogrožena zanesljivost oskrbe v posameznem sistemu;
- upravni inšpekcijski nadzor nad IBS in PDS je urejen ločeno (oboje skladno s posebnimi

zahtevami iz Direktive 2016/1148/ES). Ločeno je urejen tudi upravni inšpekcijski nadzor nad organi državne uprave.

XI. Kazenske določbe

- predlog zakona omogoča, da se za v njem določene prekrške v hitrem postopku izrekajo globe tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom;
- predpisane globe so v primerih, ko IBS in PDS ne izpolnjujeta obveznosti iz tega zakona, določene v višini, ki je učinkovita, sorazmerna in odvračalna (skladno z zahtevo iz Direktive 2016/1148/ES);
- predlog zakona ločeno ureja prekrške v primerih, ko obveznosti tega zakona ne izpolnjujejo IBS, PDS ali organi državne uprave (kaznuje se le odgovorna oseba organa državne uprave).

XII. Prehodne določbe

- prehodne določbe urejajo začetek delovanja pristojnega nacionalnega organa, ki ga določi vlada najkasneje v treh mesecih od uveljavitve tega zakona z uskladitvijo uredbe, ki ureja organe v sestavi ministrstev, z določbami tega zakona (predvidoma bo tako imenovana »Uprava RS za informacijsko varnost«), pristojni nacionalni organ pa začne z delovanjem po tem zakonu najkasneje do dne 1. januarja 2020;
- do pričetka delovanja PNO njegove naloge opravlja UVTP skladno s tem zakonom, razen nalog upravnega odločanja in nadzora, ki jih opravlja ministrstvo, pristojno za informacijsko družbo. Namreč, UVTP kot vladna služba sistemsko ne more izvajati nalog upravnega odločanja in nadzora. Zaradi odložitve pričetka delovanja PNO je potrebno zagotoviti, da se bo ZIV izvajal pred 1. januarjem 2020 v polnem obsegu in skladno z direktivo, ki se prenaša;
- prehodne določbe urejajo tudi delovanje drugih pristojnih organov, pri čemer nacionalni CSIRT z delovanjem po tem zakonu začne dne 1. januarja 2019. CSIRT organov državne uprave se vzpostavi na ministrstvu, pristojnem za upravljanje informacijsko-komunikacijskih sistemov državne uprave, do 1. januarja 2019, do njegove vzpostavitve pa njegove naloge glede obravnave incidentov izvaja nacionalni CSIRT;
- določeni so roki za sprejem konkretno naštetih obveznih podzakonskih predpisov po tem zakonu in za sprejem strategije (v skladu z določbami tega zakona);
- določeno je prehodno obdobje za določitev posameznih izvajalcev IBS, za določitev zavezanih organov državne uprave ter za izpolnjevanje obveznosti IBS, PDS in organov državne uprave.

XIII. Končna določba

- Določa začetek veljavnosti zakona − petnajsti dan po objavi v Uradnem listu RS.
- Način reševanja

Skladno z zgoraj zapisanim se s predlogom zakona v pravni red prenaša Direktiva 2016/1148/ES, katere cilj in namen je zagotoviti visoko skupno raven varnosti omrežij in informacijskih sistemov v EU. Poleg tega se bo z zakonom sistemsko uredilo področje informacijske varnosti tako na strateški kot tudi na operativni ravni nacionalnega sistema zagotavljanja informacijske varnosti, razen na področjih, ki sta izključeni. Predlog zakona se ne uporablja za operaterje, za katere veljajo posebne obveznosti glede varnosti in celovitosti omrežij iz ZEKom-1, ter za ponudnike storitev zaupanja, za

katere veljajo zahteve iz 19. člena Uredbe eIDAS.

Na podlagi predloga zakona se podzakonski predpisi iz njegovega prvega odstavka 6. člena, četrtega odstavka 7. člena, tretjega odstavka 12. člena in tretjega odstavka 17. člena sprejmejo v šestih mesecih od uveljavitve tega zakona. Poleg tega se zaradi določitve pristojnega nacionalnega organa, ki je organ v sestavi ministrstva, pristojnega za informacijsko družbo, predvideva uskladitev Uredbe o organih v sestavi ministrstev (Uradni list RS, št. 35/15, 62/15, 84/16, 41/17 in 53/17) z določbami tega zakona v treh mesecih od njegove uveljavitve. Iz razloga pravne varnosti se v enakem roku predvideva uskladitev Sklepa 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.

- Normativna usklajenost predloga zakona

Predlog zakona je usklajen z veljavno zakonodajo ter s splošno veljavnimi načeli mednarodnega prava in z mednarodnimi pogodbami, ki obvezujejo RS. Predlog zakona prenaša Direktivo 2016/1148/ES.

- Usklajenost predloga zakona

Osnutek predloga zakona je bil od 8. septembra do 9. oktobra 2017 v javni obravnavi. O javni obravnavi smo še posebej opozorili nekatere bistvene deležnike, resorje in organe ter lokalne skupnosti.

Predlog zakona je usklajen s samoupravnimi lokalnimi skupnostmi in delno s civilno družbo oziroma ciljnimi skupinami, na katere se predlog zakona nanaša, ter s predstavniki zainteresirane javnosti.

Navedba neusklajenih vprašanj izhaja iz točke 7 tega gradiva (PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA).

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNA FINANČNA SREDSTVA

Z vzpostavitvijo in delovanjem organov skladno s predlogom ZIV bodo nastale finančne posledice za državni proračun zaradi:

1. zagotovitve pogojev za delovanje pristojnega nacionalnega organa;
2. zagotovitve pogojev za delovanje CSIRT organov državne uprave na ministrstvu, pristojnem za omrežja in informacijske sisteme organov državne uprave;
3. zagotovitve pogojev za izvajanje nalog drugostopenjskega organa pri reševanju pritožb zoper odločbe, ki jih izda pristojni nacionalni organ po tem zakonu (po četrtem odstavku 21. člena, četrtem odstavku 22. člena in v postopkih nadzora) in za izvajanje nalog strokovne pomoči pri upravljanju pristojnega nacionalnega organa;
4. zagotovitve pogojev za delovanje nacionalnega CSIRT.

Pri oceni potrebnih finančnih sredstev je pri točkah 1 do 3 upoštevan letni bruto 2 znesek plače zaposlenega, skupaj s povračili stroškov in drugimi prejemki iz delovnega razmerja, v višini 30.000 eurov ter enkraten strošek vzpostavitve posameznega delovnega mesta v višini 5.000 eurov in letni strošek kasnejšega delovanja v višini 2.000 eurov na posamezno delovno mesto. V oceni je prav tako upoštevan letni strošek službenih poti in izobraževanja v višini 1.200 EUR na zaposlenega. Ker se bo ZIV predvidoma pričel izvajati sredi leta 2018, so stroški za leto 2018 temu ustrezno

prilagojeni (znižani).

Skupni ocenjeni stroški vzpostavitve in delovanja pristojnih organov skladno s predlogom ZIV:

		t	t + 1	t + 2	t + 3
	Kategorija/leto	**2018**	**2019**	**2020**	**2021**
1.	Število zaposlitev kumulativno	8	14	24	24
2.	Stroški vzpostavitve/delovanja delovnih mest	40.000 €	46.000 €	78.000 €	48.000 €
3.	Stroški plač in nadomestil (bruto 2)	120.000 €	420.000 €	720.000 €	720.000 €
4.	Službene poti in izobraževanja	6.000 €	16.800 €	28.800 €	28.800 €
5.	Investicije v strojno in programsko opremo	300.000 €	300.000 €	300.000 €	300.000 €
6.	Nakup/pridobitev prostorov	/	/	/	/
	Skupaj	**530.000 €**	**1.020.800 €**	**1.398.800 €**	**1.368.800 €**

Predlog zakona bi lahko imel posledice za druga javna finančna sredstva, katere bo mogoče oceniti po izvedbi analize tveganj, ki jih zakon v prihodnosti zahteva od posameznih zavezancev.

V nadaljevanju so podane ocene stroškov zagotovitve pogojev za delovanje po posameznih organih.

1. Zagotovitev pogojev za delovanje pristojnega nacionalnega organa:

		t	t + 1	t + 2	t + 3
	Kategorija/leto	**2018**	**2019**[1]	**2020**[2]	**2021**
1.	Število zaposlitev kumulativno	5	9	17	17
2.	Stroški vzpostavitve/delovanja delovnih mest	25.000 €	30.000 €	58.000 €	34.000 €
3.	Stroški plač in nadomestil (bruto 2)	75.000 €	270.000 €	510.000 €	510.000 €
4.	Službene poti in izobraževanja	3.750 €	10.800 €	20.400 €	20.400 €
5.	Investicije v strojno in programsko opremo	0 €	100.000 €	150.000 €	150.000 €
6.	Nakup/pridobitev prostorov	/	/	/	/
	Skupaj	**103.750 €**	**410.800 €**	**738.400 €**	**714.400 €**

Ocena temelji na projekciji končnega števila novih zaposlitev po letih, in sicer v letu 2018 pet, v letu 2019 devet ter v letih 2020 in 2021 sedemnajst zaposlitev, in pripadajočih stroških ter stroških za investicije v strojno in programsko opremo, ne vključuje pa stroškov nakupa oziroma pridobitve prostorov. V letu 2018 so za namen opravljanja nalog PNO (27. člen predloga ZIV) na UVTP, vključno z administrativno podporo (kadrovsko, finančno, pravno) predvidene štiri nove zaposlitve medtem, ko je za opravljanje nalog izdajanja odločb zavezancem predvidena ena nova zaposlitev

[1] Do konca leta 2019 UVTP kot pristojni nacionalni organ

[2] Od začetka leta 2020 naprej Uprava RS za informacijsko varnost kot pristojni nacionalni organ

na MJU. Potrebna finančna sredstva v višini 103.750 eurov za leto 2018 za dodatne pristojnosti in naloge iz tega zakona zagotovi ministrstvo, pristojno za informacijsko varnost (sedaj MJU) s svoje proračunske postavke PP170089 Razvoj, vzdrževanje in upravljanje informacijske varnosti.

V letu 2019 so za namen opravljanja nalog PNO (27. člen predloga ZIV) predvidene še tri nove zaposlitve medtem, ko je za opravljanje nalog inšpekcijskega nadzora predvidena ena nova zaposlitev na MJU. Presoja zagotovitve dodatnih zaposlitev bo izvedena v skladu s 60. členom sprejetega Zakona o izvrševanju proračuna RS za leti 2018 in 2019 ter sprejetimi sklepi Vlade RS o kadrovskih načrtih organov državne uprave.

MJU z letom 2019 priskrbi redno proračunsko postavko v sklopu razreza proračuna na nivoju ministrstva, iz katere se od leta 2020 naprej zagotavlja tudi financiranje uprave.

S pričetkom delovanja uprave 1. 1. 2020 bo nanjo iz UVTP preneseno sedem javnih uslužbencev skupaj s kvotami in finančnimi sredstvi zanje ter dva javna uslužbenca iz MJU. V letu 2020 je predvideno še osem novih zaposlitev, in sicer ena v sekretariatu MJU za podporo delovanju uprave, ena za izvajanje inšpekcijskih in nadzornih funkcij nad organi državne uprave, dva za izvajanje inšpekcijskih in nadzornih funkcij nad izvajalci bistvenih storitev in ponudniki digitalnih storitev ter štiri zaposlitve za namene opravljanja preostalih nalog PNO.

V letu 2021, ko niso predvidene nove zaposlitve, bo Uprava RS za informacijsko varnost tako imela šestnajst uslužbencev.

2. Zagotovitev pogojev za delovanje CSIRT organov državne uprave:

		t	t + 1	t + 2	t + 3
	Kategorija/leto	**2018**	**2019**	**2020**	**2021**
1.	Število zaposlitev kumulativno	2	3	4	4
2.	Stroški vzpostavitve/delovanja delovnih mest	10.000 €	9.000 €	11.000 €	8.000 €
3.	Stroški plač in nadomestil (bruto 2)	30.000 €	90.000 €	120.000 €	120.000 €
4.	Službene poti in izobraževanja	1.500 €	3.600 €	4.800 €	4.800 €
5.	Investicije v strojno in programsko opremo	300.000 €	200.000 €	150.000 €	150.000 €
6.	Nakup/pridobitev prostorov	0 €	0 €	0 €	0 €
	Skupaj	**341.500 €**	**302.600 €**	**285.800 €**	**282.800 €**

Ocena temelji na projekciji končnega števila novih zaposlitev po letih, in sicer v letu 2018 dve, v letu 2019 tri ter v letih 2020 in 2021 štiri zaposlitve, in pripadajočih stroških ter stroških za investicije v strojno in programsko opremo za obvladovanje incidentov v informacijskih sistemih in omrežjih organov državne uprave.

3. Zagotovitev pogojev za izvajanje nalog drugostopenjskega organa pri reševanju pritožb zoper odločbe, ki jih izda pristojni nacionalni organ po tem zakonu (po četrtem odstavku 21. člena, četrtem odstavku 22. člena in v postopkih nadzora) in za izvajanje nalog strokovne pomoči pri upravljanju pristojnega nacionalnega organa (organa v sestavi):

		t	t + 1	t + 2	t + 3
	Kategorija/leto	**2018**	**2019**	**2020**	**2021**
1.	Število zaposlitev kumulativno	1	2	3	3
2.	Stroški vzpostavitve/delovanja delovnih mest	5.000 €	7.000 €	9.000 €	6.000 €
3.	Stroški plač in nadomestil (bruto 2)	15.000 €	60.000 €	90.000 €	90.000 €
4.	Službene poti in izobraževanja	750 €	2.400 €	3.600 €	3.600 €
5.	Investicije v strojno in programsko opremo	0 €	0 €	0 €	0 €
6.	Nakup/pridobitev prostorov	0 €	0 €	0 €	0 €
	Skupaj	**20.750 €**	**69.400 €**	**102.600 €**	**99.600 €**

Ocena temelji na projekciji končnega števila novih zaposlitev po letih, in sicer v letu 2018 ena, v letu 2019 dve ter v letih 2020 in 2021 tri zaposlitve, in pripadajočih stroških za potrebe izvajanja nalog drugostopenjskega organa pri reševanju pritožb na podlagi tega zakona in administrativne podpore pristojnemu nacionalnemu organu (kadrovske, finančne). Uredba o organih v sestavi ministrstev (Uradni list RS, št. 35/15, 62/15, 84/16, 41/17 in 53/17), ki mora biti novelirana zaradi ustanovitve pristojnega nacionalnega organa, kot organa v sestavi ministrstva pristojnega za informacijsko družbo (sedaj MJU), v prvem odstavku 3. člena namreč določa, da ministrstvo izvaja vse naloge strokovne pomoči pri upravljanju za organ v sestavi, če je v takšnem organu v sestavi sistemiziranih manj kot 100 delovnih mest. Ker bo novi pristojni nacionalni organ, ki se bo ustanovil kot organ v sestavi resorno pristojnega ministrstva imel manj kot 100 delovnih mest, je potrebno predvideti dodatno delovno mesto za opravljanje teh nalog.

4. Zagotovitev pogojev za delovanje nacionalnega CSIRT:

		t	t + 1	t + 2	t + 3
	Kategorija/leto	**2018**	**2019**	**2020**	**2021**
1.	Stroški SI-CERT	64.000 €	238.000 €	272.000 €	272.000 €
	Skupaj	**64.000 €**	**238.000 €**	**272.000 €**	**272.000 €**

Ocena stroškov obsega vzpostavitev oziroma delovanja delovnih mest, stroške plač ter povračil stroškov in drugih prejemkov iz delovnega razmerja (bruto 2), stroške službenih poti in izobraževanja ter stroške za investicije v strojno in programsko opremo nacionalnega odzivnega centra SI-CERT na Arnes. Dodatna finančna sredstva za ta namen v letih 2018, 2019, 2020 in 2021 zagotovi MJU.

4. NAVEDBA, DA SO SREDSTVA ZA IZVAJANJE ZAKONA V DRŽAVNEM PRORAČUNU ZAGOTOVLJENA, ČE PREDLOG ZAKONA PREDVIDEVA PORABO PRORAČUNSKIH SREDSTEV V OBDOBJU, ZA KATERO JE BIL DRŽAVNI PRORAČUN ŽE SPREJET

Za izvajanje zakona so za leto 2018 zagotovljena sredstva v državnem proračunu, in sicer v okviru Ministrstva za javno upravo, projekt informacijska varnost (šifra 3130-17-0009), na proračunski postavki PP170089 – Razvoj, vzdrževanje in upravljanje informacijske varnosti. Sredstva so zagotovljena v višini 530.000 eurov.

5. PRIKAZ UREDITVE V DRUGIH PRAVNIH SISTEMIH IN PRILAGOJENOSTI PREDLAGANE UREDITVE PRAVU EVROPSKE UNIJE

Prikaz ureditve v pravnem redu EU
Predlog zakona je usklajen s pravnim redom EU.

Prikaz ureditve v najmanj treh pravnih sistemih držav članic EU
Za primerjanje stanja na področju, ki ureja ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov, v nadaljevanju predstavljamo zakonodajne rešitve treh držav, in sicer Češke republike, Zvezne republike Nemčije in predvidene rešitve Kraljevine Nizozemske.

Češka republika

V Češki republiki je v skladu z odločbo češke vlade št. 781 z dne 19. oktobra 2011 za zagotavljanje kibernetske varnosti odgovoren Nacionalni varnostni organ (v nadaljnjem besedilu: NVO). Z isto odločbo sta bila ustanovljena tudi Nacionalni center za kibernetsko varnost (v nadaljnjem besedilu: NCKV), ki je podrejen NVO, in Svet za kibernetsko varnost (v nadaljnjem besedilu: SKV).

NCKV upravlja vladni CERT, usmerja sodelovanje s skupinami CSIRT tako na nacionalni kot tudi mednarodni ravni, pripravlja varnostne standarde za različne kategorije subjektov v državi, podpira izobraževanje in dvig ozaveščenosti o kibernetski varnosti ter podpira raziskave in razvoj na področju kibernetske varnosti. NVO nadzira in redno ocenjuje delo NCKV, njegovo letno poročilo pa prouči tudi SKV ter potrdi vlada.

SKV je uradni forum za med agencijsko koordinacijo. V njem so zastopani NVO, ministrstvo za notranje zadeve, ministrstvo za obrambo, ministrstvo za zunanje zadeve, ministrstvo za finance, ministrstvo za industrijo in trgovino, ministrstvo za promet, policija, civilna notranja in zunanja obveščevalna služba, vojaška obveščevalna služba, urad za varstvo osebnih podatkov in urad za telekomunikacije. SKV lahko k sodelovanju po potrebi povabi tudi predstavnike subjektov, ki upravljajo kritično infrastrukturo, ali druge zunanje strokovnjake.

Na operativni ravni deluje vladni CERT (GovCERT.CZ), čigar glavne naloge so zbiranje priglasitev kibernetskih incidentov od določenih subjektov, njihova analiza in pomoč. Zakon o kibernetski varnosti je uvedel obveznost priglasitve kibernetskih incidentov za subjekte, ki upravljajo kritično informacijsko infrastrukturo, vladno in z njo povezano informacijsko infrastrukturo ter internetna vozlišča, ki omogočajo neposredno povezavo do kritične informacijske infrastrukture ali omrežij v tujini. Ti subjekti so dolžni izvajati preventivne varnostne ukrepe, ki segajo od zagotavljanja fizične varnosti do kriptografije, ter priglašati kibernetske incidente vladnemu CERT. Drugi ponudniki internetnih storitev priglašajo kibernetske incidente nacionalnemu CERT (trenutno CSIRT.CZ), ki opravlja storitve za zasebni sektor.

Novela zakona o kibernetski varnosti je podobno, a nekoliko širše kot Direktiva 2016/1148/ES opredelila področje izvajalcev bistvenih storitev. To sta področji energije, digitalne infrastrukture, oskrbe s pitno vodo in njene distribucije, zdravstva, prometa, bančništva, infrastrukture finančnega trga in kemične industrije. Izvajalci bistvenih storitev morajo vpeljati in izvajati varnostne ukrepe v obsegu, ki je nujen za zagotavljanje kibernetske varnosti informacijskega in komunikacijskega sistema kritične informacijske infrastrukture ter informacijskega sistema bistvene storitve, in voditi njihovo varnostno dokumentacijo. V skladu z zahtevami Direktive 2016/1148/ES so opredeljeni ponudniki digitalnih storitev, ki so dolžni vpeljati in izvajati primerne in sorazmerne varnostne ukrepe za elektronsko komunikacijsko omrežje in informacijske sisteme, ki jih uporabljajo v povezavi z zagotavljanjem svoje storitve, pri čemer ti varnostni ukrepi upoštevajo zagotavljanje varnosti informacij, obvladovanje kibernetskih varnostnih incidentov, upravljanje neprekinjenega delovanja, spremljanje, revizijo, testiranje in skladnost z mednarodnimi predpisi.

NVO lahko razglasi izredne razmere na področju kibernetske varnosti, pri čemer lahko izvajalcem bistvenih storitev naloži dodatne varnostne ukrepe. Lahko izvaja varnostne preglede in izreka kazni. NVO je pripravil tudi uredbo o kibernetski varnosti ter uredbo o pomembnih informacijskih sistemih in merilih za njihovo določitev. Uredba o kibernetski varnosti natančno določa preventivne varnostne ukrepe ter postopek priglasitve kibernetskih incidentov, tako za CSIRT.CZ kot tudi za GovCERT.CZ.

Zvezna republika Nemčija

V Zvezni republiki Nemčiji je pristojni organ in enotna kontaktna točka za informacijsko varnost Zvezni urad za informacijsko varnost (Bundesamt für Sicherheit in der Informationstechnik − BSI). BSI ocenjuje varnostna tveganja, povezana z uporabo informacijske tehnologije, in razvija preventivne varnostne ukrepe. Zagotavlja informacije o tveganjih in nevarnostih, povezanih z uporabo informacijske tehnologije, in predlaga ustrezne rešitve. To delo vključuje preizkušanje in ocenjevanje varnosti informacijskih sistemov, vključno z njihovim razvojem v sodelovanju z industrijo. Po nemškem zakonu o varnosti informacijske tehnologije (IT-Sicherheitsgesetz) BSI preverja izpolnjevanje posebnih varnostnih zahtev za ponudnike kritične infrastrukture, ki jim v primeru neizpolnjevanja zahtev lahko naloži upravne globe.

Pristojnosti na področju informacijske varnosti imajo tudi drugi organi, na primer ministrstvo za zunanje zadeve, ministrstvo za obrambo, zvezni urad za varstvo ustave, zvezna obveščevalna služba, pa tudi regulatorji v sektorjih kritične infrastrukture.

Na operativni ravni obstaja omrežje odzivnih centrov, na čelu z nacionalnim CERT (CERT-BUND). Država ima tudi dobro razvito javno-zasebno partnerstvo na področju zagotavljanja kibernetske varnosti, kot je na primer zavezništvo za kibernetsko varnost, kar se na podlagi sodelovanja kaže tudi v nacionalnih politikah in pravnem okviru.

Zakonodaja ureja obveznosti družb − upravljavcev kritične infrastrukture; ti morajo zagotoviti ustrezne organizacijske in tehnične ukrepe za preprečevanje incidentov, ki vplivajo na razpoložljivost, celovitost, verodostojnost in zaupnost njihovih informacijskih sistemov, sestavnih delov teh sistemov ali procesov, ki lahko vodijo do okvare ali poslabšanja ali lahko povzročijo odpoved ali poslabšanje funkcionalnosti kritične infrastrukture. Z že obstoječo zakonodajo so opredeljeni sektorji kritične infrastrukture, sektorji energetike, informacijske tehnologije in telekomunikacij, transporta, zdravstva, vode, hrane ter finančnih in zavarovalniških storitev.

Upravljavci kritične infrastrukture morajo incidente priglasiti BSI. V redkih primerih reguliranih sektorjev obstajajo dodatne obveznosti glede obveščanja o kršitvi varnosti v sektorskih zakonih. Na primer, ponudnik javnega telekomunikacijskega omrežja ali javno dostopnih telekomunikacijskih storitev mora sektorskega regulatorja BNetzA obvestiti o morebitni kršitvi informacijske varnosti. Če za družbo velja več kot ena obveznost priglasitve kršitve varnosti ali podobne obveznosti razkritja (na primer ad hoc priglasitev v primeru družbe, ki kotira na borzi), mora obstajati interni postopek priglasitve, s katerim se sinhronizira vse potrebne priglasitve in prepreči odstopanja v njih.

Vsaka družba v Nemčiji je odgovorna za nastalo škodo, ki bi se ji bilo mogoče izogniti z zagotovitvijo razumne ravni informacijske varnosti, če torej zaradi malomarnosti ni izvedla potrebnih varnostnih ukrepov in aktivnosti. To splošno pravilo velja ne glede na vrsto izdelkov ali storitev, ki jih družba zagotavlja.

Čeprav sedanja nemška zakonodaja že opredeljuje nekatere sektorje kritične infrastrukture in varnostne zahteve za organe in organizacije, pa bo tako kot v večini držav članic za usklajenost z Direktivo 2016/1148/ES zakonodajo treba še dopolniti.

Kraljevina Nizozemska

Na Nizozemskem je individualna in kolektivna odgovornost za zagotavljanje kibernetske varnosti porazdeljena med več kot 20 organi v javnem in zasebnem sektorju. Koordinacijo vseh aktivnosti in organov izvaja leta 2011 ustanovljen Svet za kibernetsko varnost, ki deluje na strateški ravni sistema. V javnem sektorju so vključena ministrstva za varnost in pravosodje, za notranje zadeve in odnose v kraljevini, za gospodarstvo, za obrambo, za zunanje zadeve ter za raziskave, izobraževanje in znanost. Prav tako so vključeni policija, državno tožilstvo, fiskalna obveščevalna in preiskovalna služba, inšpektorat za varnost in pravosodje, obveščevalna in varnostna služba, agencija za varstvo podatkov, sektorski regulativni organi (na primer za telekomunikacije) ter centralna banka. V sistemu sodelujejo tudi regionalne in lokalne oblasti.

Sektorje izvajalcev bistvenih storitev pokrivajo različni pristojni organi. Ministrstvo za gospodarstvo je pristojno za sektorja energija in digitalna infrastruktura. Banka Nizozemske je pristojna za sektorja bančništvo in infrastruktura finančnega trga. Ministrstvo za infrastrukturo in okolje je pristojno za sektorja promet in oskrba s pitno vodo in njena distribucija, ministrstvo za zdravje, blaginjo in šport pa za sektor zdravstvo.

Večina odgovornosti za zagotavljanje kibernetske varnosti v zasebnem sektorju je naložena finančnemu sektorju (poslovne banke, nizozemsko združenje bank in nizozemska platforma za elektronsko poslovanje) ter izvajalcem bistvenih storitev. Nekatere odgovornosti zahtevajo sodelovanje poslovne skupnosti na splošno. Akademski svet je vključen prek Nizozemske organizacije za znanstveno raziskovalno dejavnost in prek vladnega financiranja neodvisnih raziskovalnih organov, kot je Nizozemska organizacija za aplikativne znanstvene raziskave.

Svet za kibernetsko varnost poleg koordinacije sodelujočih organov in organizacij tudi svetuje vladi in organizacijam iz zasebnega sektorja o razvoju na področju kibernetske varnosti, postavlja prioritete pri obravnavi groženj za informacijsko komunikacijsko tehnologijo (IKT), ocenjuje potrebe na področju raziskav in razvoja ter skrbi za prenos znanja.

Na operativni ravni sistema skrbi za obravnavo kibernetskih incidentov Nacionalni center za kibernetsko varnost (NCKV), v katerega je bil integriran tudi vladni CERT (GOVCERT.NL). NCKV ima ključno vlogo v javno-zasebnem omrežju kibernetske varnosti in deluje kot varnostno-operativni center na področju ozaveščanja, odpornosti, prepoznavanja, opozarjanja, poročanja in kriznega upravljanja ter svetovanja strankam iz zasebnega in javnega sektorja. NCKV, ki je podrejen nacionalnemu koordinatorju za proti terorizem in varnost na ministrstvu za varnost in pravosodje, pomaga tako vladi kot tudi organizacijam iz javnega in zasebnega sektorja, ki so odgovorne za kritično infrastrukturo, ter poskuša okrepiti javno-zasebna partnerstva. S tem namenom je bil ustanovljen tudi IKT-odbor za odzivanje, javno-zasebno partnerstvo, ki povezuje telekomunikacijska podjetja, ponudnike energije, banke in vladne organe. Odbor se aktivira v primeru večjih motenj v IKT z nalogo svetovanja nacionalnim organom pri ukrepih za obvladovanje kriz.

Izjava o skladnosti predloga zakona s pravnimi akti EU in korelacijska tabela pri prenosu direktive sta priloženi.

6. PRESOJA POSLEDIC, KI JIH BO IMEL SPREJEM ZAKONA
6.1 Presoja administrativnih posledic
a) V postopkih oziroma poslovanju javne uprave ali pravosodnih organov

Glede predlagane ustanovitve pristojnega nacionalnega organa kot novega organa v sestavi ministrstva, pristojnega za informacijsko družbo, in reorganizacije nacionalnega sistema informacijske varnosti na podlagi tega zakona pojasnjujemo:

Vlada RS je dne 6. aprila 2017 sprejela Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov (UVTP) (Uradni list RS, št. 17/17). S tem sklepom so bile določene strokovne naloge in organizacija UVTP na področju kibernetske varnosti. UVTP je tako v okviru nacionalnega sistema informacijske varnosti postal tudi pristojni organ na strateški ravni. Na operativni ravni sistema pa so zmogljivosti za odzivanje na incidente v kibernetskem prostoru porazdeljene med SI-CERT kot nacionalni odzivni center za omrežne incidente, Sektor za informacijsko varnost v okviru Direktorata za informatiko na Ministrstvu za javno upravo (MJU), Ministrstvo za obrambo (MO) za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Slovensko obveščevalno-varnostno agencijo (SOVA) na področju protiobveščevalnega delovanja ter Policijo, Urad za informatiko in telekomunikacije in Upravo kriminalistične policije, predvsem Center za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala. Organi na obeh ravneh sistema so podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju.

RS do zdaj ni imela zakonsko urejenega področja zagotavljanja informacijske varnosti. Naraščajoči trend obsega incidentov v kibernetskem prostoru in velika odvisnost gospodarstva ter celotne družbe od neprekinjenega delovanja omrežij in informacijskih sistemov pa zahtevajo celovito ureditev in tudi okrepitev področja zagotavljanja informacijske varnosti. Državo k temu zavezujejo tudi sprejeti strateški domači in mednarodni dokumenti, na primer Resolucija o strategiji nacionalne varnosti RS, Strategija kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor« ter lansko leto sprejeti nacionalna Strategija kibernetske varnosti in predvsem Direktiva

2016/1148/ES, ki se prenaša s predlogom tega zakona.

Glede na zgoraj navedeno potrebnih nalog in pristojnosti ni mogoče celovito in sistemsko izvajati v nobenem od zgoraj navedenih organov, saj je za dosego ciljev na področju informacijske varnosti treba zagotoviti ustrezno koordinacijo med vsemi resorji in organi ter za to ustanoviti nov organ – pristojni nacionalni organ, ki je organ v sestavi ministrstva, pristojnega za informacijsko družbo (predvidoma tako imenovana »Uprava RS za informacijsko varnost«). Le-ta bo skladno s prehodnimi določbami predloga tega zakona z dnem začetka delovanja od UVTP prevzel naloge, arhive in dokumentacijo, ki se nanašajo na kibernetsko varnost, ter javne uslužbence, pravice proračunske porabe, opremo in druge zbirke podatkov oziroma evidence iz prevzetega delovnega področja. Vlada pa bo uskladila sklep o ustanovitvi, nalogah in organizaciji UVTP z določbami tega zakona. Ob tem je treba pojasniti, da bo pristojni nacionalni organ izvajal naloge, ki jih UVTP kot vladna služba sistemsko ne more prevzeti, saj bo med drugim v upravnem postopku odločal o sprejemu ukrepov na podlagi tega zakona, izvajal pa bo tudi inšpekcijski nadzor nad izvajanjem njegovih določb ter na njegovi podlagi sprejetih predpisov ter odločb.

Glede nacionalnega CSIRT je treba pojasniti, da ne gre za ustanovitev novega organa, saj je predvideno, da je to odzivni center SI-CERT pri Arnes, ki pa bo zaradi obširnih nalog, ki jih bo skladno s tem zakonom začel izvajati s 1. januarjem 2019, moral biti okrepljen.

Glede CSIRT organov državne uprave, ki mora biti v skladu z zahtevami tega zakona vzpostavljen, na ministrstvu, pristojnem za upravljanje informacijsko-komunikacijskih sistemov državne uprave, najkasneje do 1. januarja 2019, pojasnjujemo, da je njegova vzpostavitev potrebna zaradi nacionalnih določb predloga tega zakona, ki poleg zavezancev, ki izhajajo iz Direktive 2016/1148/ES (izvajalci bistvenih storitev in ponudniki digitalnih storitev), za zavezance določa še tretjo kategorijo, in sicer organe državne uprave. Za celovito in sistemsko ureditev informacijske varnosti v RS je poleg obveznosti, ki jih nalaga Direktiva 2016/1148/ES, iz nacionalnih razlogov treba urediti tudi to področje.

Tak zaključek glede CSIRT organov državne uprave je potreben, kljub delni ureditvi zadevnega področja v zakonu, ki ureja državno upravo, in tam predvidenem podzakonskem predpisu. Pri tem gre za določbe o upravljanju informacijsko-komunikacijskih sistemov državne uprave iz zakona, ki ureja državno upravo, in predpisa, ki ga na tej podlagi sprejme vlada glede določitve podatkovnih in tehnoloških standardov, smernic za skupne informacijske rešitve in skupne varnostne politike. Predlog tega predlog tega zakona ne posega v prej navedene predpise, določa le dodatne obveznosti za organe državne uprave, vendar z vidika zmanjšanja administrativnih ovir dopušča, da lahko organi državne uprave že izdelano varnostno dokumentacijo na podlagi drugih predpisov, dopolnijo skladno s tem zakonom.

Predlog zakona sicer prinaša nekatere obveznosti za organe državne uprave, ki so zavezanci po tem zakonu, saj bodo morali poskrbeti za ustrezno raven varnosti svojih omrežij in informacijskih sistemov, skladno s tem zakonom, pa tudi nekatera administrativna bremena zaradi priglasitve incidentov CSIRT organov državne uprave in sodelovanja z njim ter pristojnim nacionalnim organom. Vendar bo v končni posledici upoštevanje določb predloga zakona izboljšalo informacijsko varnost zavezanih organov državne uprave in s tem zmanjšalo njihovo ranljivost v primeru različnih incidentov ali kibernetskega napada, ki bi sicer lahko pri njih povzročili večjo škodo. Prav tako se bodo ob ustrezni priglasitvi incidentov na CSIRT organov državne uprave in ob

sodelovanju z njim in s pristojnim nacionalnim organom zmanjšali že nastali negativni vplivi incidentov. Posledično bo večja informacijska varnost zavezanih vplivala tudi na zaupanje uporabnikov in njihovo uporabo storitev organov državne uprave.

b) Pri obveznostih strank do javne uprave ali pravosodnih organov

Predlog zakona ne bo imel posledic pri obveznostih strank do javne uprave ali pravosodnih organov.

6.2 Presoja posledic za okolje, vključno s prostorskimi in varstvenimi vidiki

Predlog zakona ima pozitivne posledice za okolje, za cilje upravljanja voda in za varstvo pred naravnimi in drugimi nesrečami s posledicami za okolje, kot tudi za zmanjševanje verjetnosti in stopnje tveganja za okolje.

Predlog zakona namreč med področja, na katerih delujejo izvajalci bistvenih storitev (zavezanci po tem zakonu), uvršča tudi področje za oskrbo s pitno vodo in njeno distribucijo ter varstvo okolja. S tem ko bodo izvajalci bistvenih storitev iz omenjenih področij poskrbeli za ustrezno raven varnosti svojih omrežij in informacijskih sistemov skladno s tem zakonom, se bo zmanjšala njihova ranljivost v primeru različnih incidentov ali kibernetskega napada, ki bi sicer lahko imeli negativne posledice za obe področji. Prav tako se bodo ob ustrezni priglasitvi incidentov nacionalnemu CSIRT in ob sodelovanju z njim ter pristojnim nacionalnim organom lahko zmanjšali tudi že nastali negativni vplivi incidentov na obe področji.

6.3 Presoja posledic za gospodarstvo

Predlog zakona ima vpliv na gospodarstvo, saj so med zavezanci lahko tudi gospodarski subjekti. Po predlogu zakona so izvajalci bistvenih storitev (kot ena izmed skupin zavezancev) namreč lahko javni ali zasebni subjekti, ki spadajo v katerega od v zakonu določenih področij: energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo in infrastruktura finančnega trga, preskrba s hrano in varstvo okolja.

Poleg tega so ponudniki digitalnih storitev (skupina zavezancev po zakonu) lahko le gospodarski subjekti, s tem da so izključen ponudniki digitalnih storitev glede na kriterije, ki ustrezajo opredelitvi mikro in majhnih podjetij kot so opredeljena v Direktivi 2016/1148/ES, ki se pri tem neposredno sklicuje na priporočilo EK .

Predlog zakona sicer prinaša nekatere obveznosti za tiste gospodarske subjekte, ki so zavezanci po tem zakonu, saj bodo morali poskrbeti za ustrezno raven varnosti svojih omrežij in informacijskih sistemov skladno s tem zakonom, pa tudi določena administrativna bremena zaradi priglasitve incidentov nacionalnemu CSIRT in sodelovanja z njim ter pristojnim nacionalnim organom.

Administrativna bremena so pri izvajalcih bistvenih storitev omejena tudi tako, da lahko le-ti ob upoštevanju varnostnih zahtev druge področne zakonodaje področij, svojo že izdelano dokumentacijo (le) dopolnijo skladno s tem zakonom.

Upoštevanje določb predloga zakona bo izboljšalo informacijsko varnost zavezancev in s tem zmanjšalo njihova ranljivost v primeru različnih incidentov ali kibernetskega napada, ki bi sicer lahko imela tudi večje škodljive posledice za njih. Prav tako se bodo ob ustrezni priglasitvi incidentov nacionalnemu CSIRT in ob sodelovanju z njim ter pristojnim nacionalnim organom zmanjšali že nastali negativni vplivi incidentov. Posledično bo predlog zakona zaradi večje informacijske varnosti zavezancev iz gospodarstva izboljšal njihovo konkurenčnost, tako v nacionalnem kot v mednarodnem gospodarskem prostoru.

Večja informacijska varnost izvajalcev bistvenih storitev, zavezancev iz gospodarstva, bo hkrati imela pozitiven vpliv na potrošnike in gospodinjstva, saj bo s tem zagotovljena večja zanesljivost storitev teh zavezancev.

6.4 Presoja posledic za socialno področje

Predlog zakona bo imel pozitivne posledice za socialno okolje, saj se bo zagotavljanju informacijske varnosti namenilo več pozornosti, hkrati se bo okrepilo zaupanje v informacijsko varnost ter s tem v storitve izvajalcev bistvenih storitev in ponudnikov digitalnih storitev. Ob tem lahko predlog zakona pozitivno vpliva na zaposlenost in trg dela, saj lahko ustvari nova delovna mesta za strokovnjake s področja informacijske varnosti.

6.5 Presoja posledic za dokumente razvojnega načrtovanja

Ukrepi iz predloga zakona bodo pripomogli k uresničevanju ciljev že sprejetih strateških domačih in mednarodnih dokumentov, na primer Resolucije o strategiji nacionalne varnosti Republike Slovenije, Strategije kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor« in leta 2016 sprejete nacionalne Strategije kibernetske varnosti ter Direktive 2016/1148/ES.

Zaradi uskladitve z Direktivo 2016/1148/ES predlog zakona prinaša še nekatere dodatne elemente, ki jih bo treba vključiti v veljavno Strategijo kibernetske varnosti, zaradi česar se v prehodnih določbah predvideva sprejem strategije (skladno s tem zakonom) v roku enega leta od njegove uveljavitve.

6.6 Presoja posledic za druga področja
/

6.7 Izvajanje sprejetega predpisa

a) Predstavitev sprejetega zakona

Sprejeti zakon bo objavljen na spletnih straneh Ministrstva za javno upravo.

b) Spremljanje izvajanja sprejetega predpisa

Sprejeti zakon bo v večjem delu izvajal pristojni nacionalni organ, ki bo tudi spremljal njegovo izvajanje.

Inšpekcijski nadzor bo izvajal pristojni nacionalni organ.

Ministrstvo, pristojno za informacijsko družbo, bo moralo v šestih mesecih od uveljavitve zakona izdati z zakonom predvidene pravilnike.

6.8 Druge pomembne okoliščine v zvezi z vprašanji, ki jih ureja predlog zakona
/

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA

Osnutek predloga Zakona o informacijski varnosti (ZIV) je bil 8. septembra 2017 predložen v javno obravnavo, v katero so bile vključene strokovna in zainteresirana javnost ter druge javnosti. Gradivo osnutka predloga je bilo objavljeno na državnem portalu Republike Slovenje, e-uprava, v rubriki e-demokracija (https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=8587), ter na spletnih straneh MJU (http://www.mju.gov.si/si/delovna_podrocja/informacijska_druzba/javne_objave_predlogi/), z rokom za oddajo pripomb do 9. oktobra 2017. Hkrati so bili o javni obravnavi osnutka predloga ZIV še posebej obveščeni nekateri deležniki, kot tudi nekateri organi državne uprave in resorji ter združenja oziroma skupnosti lokalne samouprave, in sicer:

Javna agencija Republike Slovenije za energijo (AGEN RS), Agencija za komunikacijska omrežja in storitve RS (AKOS), Banka Slovenije (BS), Gospodarska zbornica Slovenije (GZS), Informacijski pooblaščenec RS (IP), SI CERT, Slovenska obveščevalno-varnostna agencija (SOVA), Urad Vlade za varovanje tajnih podatkov (UVTP), Združenje bank Slovenije (ZB), Policija, Ministrstvo za finance (MF), Ministrstvo za gospodarski razvoj in tehnologijo (MGRT), Ministrstvo za infrastrukturo (MzI), Ministrstvo za izobraževanje, znanost in šport (MIZŠ), Ministrstvo za notranje zadeve (MNZ), Ministrstvo za obrambo (MO), Ministrstvo za okolje in prostor (MOP), Ministrstvo za pravosodje (MP), Ministrstvo za zdravje (MZ) in Ministrstvo za zunanje zadeve (MZZ). Skupnost občin Slovenije (SOS), Združenje občin Slovenije in Združenje mestnih občin so bili hkrati z dopisom, s katerim so bili obveščeni, da poteka javna obravnava osnutka ZIV, tudi naprošeni, da z javno obravnavo in možnostjo podaje pripomb seznanijo še druge morebitne zainteresirane deležnike z njihovega področja dela, za katere menijo, da bi jih predvidena ureditev lahko zadevala.

Mnenja, predloge in pripombe so v javni obravnavi (brez omejitev v zvezi z zaupnostjo gradiva) dali:

AGEN RS, AKOS, Akademska in raziskovalna mreža Slovenije (ARNES), Agencija za trg vrednostnih papirjev (ATVP), BS, Inštitut za korporativne varnostne študije (ICS), IP, Microsoft družba za računalniške programe in opremo d.o.o. (MICROSOFT), MF, MGRT, MIZŠ, MNZ, MO, MP, Plinovodi d.o.o. (PLINOVODI), GZS - Sekcija operaterjev elektronskih komunikacij (SOEK), SOVA, SOS, ZB, Zveza slovenskih častnikov (ZSČ) in posamezniki TV, BK, MK, SŠ, M ter en nepodpisan posameznik (NN).

Mnenja, predlogi ter pripombe so bili upoštevani v pretežni meri oziroma delno kakor sledi:

- splošna pripomba BS, TV za spremembo imena zakona ni bila upoštevana, ker predlog zakona vsebuje tudi specifične nacionalne določbe, ne gre le za prenos Direktive 2016/1148/ES;

- pripombe posameznika TV z vidika boljše jasnosti določenih zakonskih dikcij so bile v največji možni meri v okviru prostora, ki ga daje Direktiva 2016/1148/ES, ter preostali nacionalni predpisi,

pretežno upoštevane;

- na splošno pripombo ATVP, da ni jasen »obseg« ZIV oziroma ni jasno, na kak manj oziroma bolj širok nabor subjektov s področja »infrastrukture finančnega trga«, za nadzor katerih je pristojna ATVP, se bo ZIV sploh nanašal, pojasnjujemo, da bo to določila vlada najprej z določitvijo seznama bistvenih storitev, nato pa bo posebej določila še posamezne IBS (glej 6. člen);

- splošna pripomba ICS, da je potrebno med seboj nujno terminološko in vsebinsko uskladiti Zakona o informacijski varnosti in Zakon o kritični infrastrukturi je bila upoštevana v največji možni meri. Popolno vsebinsko in terminološko prekrivanje predloga ZIV in zakona, ki ureja kritično infrastrukturo, pa ni možno niti dopustno. V takšnem primeru namreč dveh ločenih zakonov sploh ne bi potrebovali. Zakona urejata različno vsebino, pri čemer predlog ZIV prenaša tudi Direktivo 2016/1148/ES, ki je zakon, ki ureja kritično infrastrukturo seveda ne upošteva;

- na splošno pripombo Agen RS odgovarjamo, da Direktiva 2016/1148/ES nobenega področja IBS posebej ne izpostavlja oziroma mu daje večje pomembnosti, zato pripombe nismo upoštevali;

- splošne pripombe SOEK glede uporabe zakona pojasnjujemo, da so operaterji v delu, ko nastopajo kot operaterji omrežja oziroma izvajajo javne komunikacijske storitve (skladno z Zakonom o elektronskih komunikacijah, kjer so določbe glede zagotavljanja varnosti omrežij in storitev ter celovitosti omrežij vsebovane v njegovem VII. poglavju), v celoti izvzeti iz obveznosti tega predloga zakona. Na pripombe, da določeni pojmi niso dovolj jasno definirani pojasnjujemo, da nekatere opredelitve sledijo Direktivi 2016/1148/ES, druge, ki so nacionalne narave, pa smo skušali čimbolj jasno opredeliti. Pripombe SOEK glede določitve PNO in njihovih pristojnosti, ki je bila v osnutku za javno obravnavo po mnenju SOEK še nedorečena, je sedaj jasnejša. Pojasnjujemo tudi, da je bila opravljena uskladitev z vsemi relevantnimi predpisi s predmetnega področja (tudi z Zakonom o kritični infrastrukturi);

- splošne pripombe ARNES so bile upoštevane;

- pripombe AVTP k 2. členu, da se (razen obveznosti glede priglasitve) določbe zakona ne uporabljajo za tiste IBS, ki imajo veljaven certifikat po standardu za sistem upravljanja informacijske varnosti ISO/IEC 27001 oziroma veljaven certifikat po drugem evropskem ali mednarodno sprejetem standardu s področja informacijske varnosti, niso bile upoštevane, saj določbe Direktive 2016/1148/ES tega ne dopuščajo niti ni primerno, da se z vidika tehnološke nevtralnosti izrecno ne omenja standardov, se pa uporaba evropskih in mednarodnih standardov vzpodbuja, kar je izrecno navedeno v 19. členu tega predloga zakona;

- pripombe ICS k 2. členu glede smiselnosti dikcij, ki so zapisane v 2. členu in opredeljujejo namen in področje uporabe zakona, smo upoštevali na način, da člen prenaša le obvezne določbe Direktive 2016/1148/ES;

- pripomba BS k 2. členu v smislu, da iz določbe osmega odstavka ni mogoče razbrati razloga, zakaj predlagatelj upošteva specialnost področne ureditve glede zahteve po zagotavljanju varnosti omrežij in sistemov ter prijave incidentov, zgolj v zvezi z ureditvijo, ki izhaja iz EU predpisov (neposredno ali zaradi prenosa), ne pa morebiti specialne ureditve, ki je določena z (drugo) nacionalno zakonodajo, ni bila sprejeta iz razloga, ker to ne bi bilo skladno z Direktivo 2016/1148/ES. Vsak zavezanec mora pregledati ali že ustreza zahtevam iz predloga tega zakona

(ne glede na kakšni pravni podlagi je sprejel ukrepe). V kolikor oceni, da že izpolnjuje vse obveznosti, ki mu jih nalaga ta predlog zakona (ne glede na kateri podlagi jih je sprejel), mu ni potrebno samo zaradi predloga tega zakona *pro forma* sprejemati nobenih dodatnih ukrepov/dokumentacije. Če pa obveznostim zadosti le delno, potem ukrepe dopolni v delu, kjer ni skladen z ZIV (glej četrti odstavek 12. člena tega zakona);

- pripombi SOEK k 2. členu ni bila upoštevana, v primeru upoštevanja bi prišlo do neskladnosti z Direktivo 2016/1148/ES (njen 1. člen);

- pripombe BS k 4. členu glede opredelitve pojma »nadzorni organ«, ki naj vključuje vsaj BS oziroma ECB, kadar je pristojna za nadzor nad bankami, ter ATVP in Agencijo za zavarovalni nadzor, kot pristojne organe za nadzor nad ponudniki infrastrukture finančnega trga, ni bila upoštevana iz razloga, ker je v predlogu zakona določen enoten nadzorni organ ne glede na kategorijo zavezanca. Pristojnost morebitnih drugih nadzornih organov nad določenimi kategorijami zavezancev, ki izvirajo iz drugih pravnih podlag, pa ostaja. Glede pripomb glede nekonsistentnega poimenovanja nekaterih izrazov ter njihove pomanjkljive pojasnjenosti, uporabe kratice CSIRT, pojasnjujemo, da le-te sledijo Direktivi 2016/1148/ES, v kolikor pa so nacionalne narave, pa smo poskušali biti z vidika jasnosti čimbolj določni. Glede uporabe angleškega poimenovanja pri kratici CSIRT pa navajamo, da uporaba angleškega jezika v zakonskem besedilu ni dopustna (je pa to dopolnjeno v obrazložitvah);

- na vprašanja s strani ZB k 4. členu pojasnjujemo, da skladno z Direktivo 2016/1148/ES pod področje (sedaj termin sektor zamenjan s »področjem«) digitalna infrastruktura zapadejo le stičišča omrežij, domenski strežniki in register domenskih imen najvišje ravni, kot to določa Priloga II (pri 7. področju- digitalna infrastruktura). Na vprašanje glede opredelitve incidentov odgovarjamo, da gre pri opredelitvi incidenta za prenos Direktive 2016/1148/ES (7. točka 4. člena), ki ne govori o škodi, temveč o dejanskem učinku na varnost. Pojasnjujemo, da opredelitve iz predloga zakona sledijo Direktivi 2016/1148/ES (opredelitve v njenem 4. členu) in jih posledično predlog zakona mora vsebovati, tiste, ki so nacionalne narave, pa smo poskušali v največji možni meri izboljšati ob upoštevanju pripomb relevantnih deležnikov;

- na pripombe TV, SOEK in posameznika TV k 4. členu pojasnjujemo, da smo nekatere njihove predloge upoštevali, glede drugih pa pojasnjujemo, da opredelitve sledijo Direktivi 2016/1148/ES (opredelitve v njenem 4. členu) in jih posledično predlog zakona mora vsebovati, tiste, ki so nacionalne narave, pa smo poskušali v največji možni meri izboljšati ob upoštevanju pripomb relevantnih deležnikov;

- pripombe posameznika TV k 4. členu (tudi k 18. členu), naj se iz zakona izloči kibernetsko obrambo, ni bila upoštevana. Ocenjeno je bilo, da je kibernetsko obrambo (je celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju) z vidika javne varnosti potrebno obdržati;

- pripomba TV k 4. členu, naj se definira »kritično infrastrukturo« ni bila upoštevana, ker je to stvar zakona, ki ureja kritično infrastrukturo;

- splošno pripombo BS k II. Poglavju- Zavezanci, da se v predlogu zakona izrecno določi, da se zahteve v zvezi z varnostjo omrežij in glede poročanja incidentov ne uporabljajo za BS kot zavezanca, nismo upoštevali iz razloga, ker Direktiva 2016/1148/ES izrecno zahteva vključitev

področja bančništvo (konkretne zavezance tudi iz področja bančništvo pa bo določila vlada skladno s 6. členom na podlagi meril in metodologije iz 7. člena tega predloga zakona);

- splošna pripomba ZSČ k II. poglavju, da naj se doda nov člen, ki naj določi pristojnosti in odgovornosti kontaktne osebe za informacijsko varnost zavezanca, ni bila sprejeta, saj menimo, da je to prepodrobno za zakonsko urejanje, je namreč stvar operative;

- na pripombe ICS k 5. členu, da bi merila in metodologija bila enotno predpisana v Zakonu o kritični infrastrukturi (ZKI), ki vsebuje tudi področje informacijsko-komunikacijske tehnologije in jih ne bi bilo smiselno različno opredeljevati za vsako pod področje v posebnem zakonu, odgovarjamo, da gre za prenos Direktive 2016/1148/ES, ki je pa ZKI ne prenaša. Pri oblikovanju metodologije za določitev IBS, ki bo poskušala biti čimbolj določno konkretizirana z uredbo, si bomo pomagali tudi z ZKI;

- pripomba AVTP k 5. členu je bila upoštevana;

- na pripombo posameznika M k 5. členu, da se pripravi tipske strukture za različne scenarije napadov (zdravstvo, promet, bančništvo, …), kateri nato sledi šablonska izvedba uredbe, odgovarjamo, da je priprava varnostnega načrta stvar vsakega posameznega zavezanca, izpolnjevati pa mora vse zakonsko določene kriterije;

- na pripombe ZB k 5. členu, naj bo seznam zavezancev zaupen in ne javno objavljen, odgovarjamo, da vodenje in vsebino seznamov sedaj določa 25. člena predloga zakona, prav tako drugi odstavek 3. člena predloga zakona določa kateri podatki se obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost (niso vsi podatki *a priori* tajni in poslovna skrivnost);

- pripombe BS k 6. členu, da se pooblastilo vladi za podrobnejšo ureditev metodologije za določanje IBS dopolni, da bo vključevalo tudi podrobnejšo ureditev pravil glede določanja ključnih, krmilnih in nadzornih informacijskih sistemov, bodo okvirno upoštevane v uredbi, podrobneje pa se jih ne da enotno določiti, saj ima vsako področje svoje specifike;

- pripombe ZB k 6. členu glede geografske razširjenosti nismo upoštevali, ker geografsko območje načeloma ni določeno, treba je upoštevati tudi čezmejni vpliv;

- glede pripomb k III. Poglavju- Informacijska varnost IBS, 8. člen, ki so jih podali ATVP, ZSČ, ZB, SOEK, posamezniki SŠ, M in TV; pripomb k IV. Poglavju- Informacijska varnost PDS, 9. člen, ki so jih podali ZSČ, ZB, BS, SOEK, posameznika M in TV; pripomb k V. Poglavju- Varnostna dokumentacija in varnostni ukrepi, 11. in 12. člen, ki so jih podali BS, posameznika SŠ in TV (k 11. členu) ter ICS, ZCČ, IP, MICROSOFT, BS, ZB in posameznika MK in TV (k 12. členu) odgovarjamo, da predlog zakona sedaj loči obveznosti glede zagotavljanja informacijske varnosti (tako glede varnostnih zahtev, varnostne dokumentacije in varnostnih ukrepov ter priglasitve incidentov) s strani zavezancev tega zakona glede na njihovo kategorijo. III. Poglavje tako opredeljuje informacijsko varnost IBS, IV. Poglavje informacijsko varnost PDS in V. Poglavje informacijsko varnost državnih organov (gre za člene od 11 do vključno 18), s katerim se je tako zadostilo določbam Direktive 2016/1148/ES ter nekaterim nacionalnim specifikam (obveznosti državnim organov), ob tem pa so bile tudi upoštevane nekatere pripombe navedenih deležnikov;

- pripombe ZČS k 8. členu glede priglasitve so bile delno upoštevane v sklopu 13. člena, njegov prvi

odstavek primeroma navaja katere incidente je potrebno priglasiti, katere informacije ter katere kriterije pri določitvi pomembnosti incidenta je potrebno upoštevati;

- pripombe posameznika S.Š. k 8. členu glede individualnega obveščanja vseh oškodovanih posameznikov, ki se lahko ob zavedanju incidenta bolje obranijo pred posledicami, nismo upoštevali, saj je nemogoče zajeti vse prizadete, menimo, da splošno obvestilo zadošča (obveščanje javnosti določa osmi in deveti odstavek 13. člena);

- na pripombe posameznika M k 8. členu odgovarjamo, da je glede varnostnih zahtev in priglasitev incidentov potrebno upoštevati določbe Direktive 2016/1148/ES in vidik sorazmernosti ter posledično ne- nalaganja prevelikih stroškov zavezancev. Določba temelji na samoregulaciji IBS, saj sami najbolj poznajo tehnološko organizacijske procese svojega specifičnega sistema, nadzor pa izvaja inšpektor. Določbe glede obveznega pen-test-a bi bila z vidika stroškov zavezancev prekomerna, niti tega ne zahteva Direktiva 2016/1148/ES, enako velja glede morebitnih izvedb avtoriziranega napada na omrežje. Vključitev formularjev pri najavi incidentov niso stvar zakonske materije, ampak v domeni organov, ki sprejemajo najavo incidentov kot pomoč na spletnih straneh, za kar menimo da je dobra rešitev. V 19. členu pa je PNO dana naloga, da spodbuja uporabo evropskih ali mednarodno sprejetih standardov in specifikacij. Menimo, da so določbe glede priglasitve incidentov s strani IBS sedaj jasnejše (posameznik je menil, da 8. člen ni dovolj jasen) tudi glede sodelovanja pristojnih organov in medsebojnega obveščanja, ravnanja z podatki in informacijami. Glede smotrnosti šestega odstavka pojasnjujemo, da so posledice incidentov lahko različne (od najmanj invazivnih do zelo hudih), vsakokratni varnostni načrt mora zato vsebovati možnosti za zmanjšanje verjetnosti incidenta oziroma njegovega učinka (kamor spada tudi ohranitev revizijske sledi oziroma »log fileov«);

- pripombe SOEK k tretjemu odstavku 8. člena so bile delno upoštevane;

- pripombe ZB k petemu odstavku 8. člena glede obveznosti prijave kaznivih dejanj s strani oseb zasebnega prava so bile upoštevane;

- pripombe ZČS k 9. členu glede priglasitve so bile delno upoštevane v sklopu 14. člena, ki določa katere incidente je potrebno priglasiti, katere informacije ter katere kriterije pri določitvi pomembnosti incidenta je potrebno upoštevati;

- pripombe BS k četrtemu odstavka 9. člena je bila upoštevana na način, da smo z vidika jasnosti izboljšali dikcijo, ki jo sedaj vsebuje šesti odstavek 14. člena (jasneje zapisano, da je obveznost priglasitve na IBS), hkrati pojasnjujemo, da gre pri šestem odstavku 14. člena za prenos petega odstavka 16. člena Direktive 2016/1148/ES;

- pripombe posameznika M k 9. členu, da se nalaga PDI izvedba pen- testov ni bila upoštevana- tega ne nalaga Direktiva 2016/1148/ES niti ni smotrno z vidika nalaganja prekomernih stroškov PDS. 4. odstavek 9. člena, k kateremu je posameznik podal pripombe, je sedaj preko določbe šestega odstavka 14. člena tega predloga zakona izboljšan in sledi Direktivi 2016/1148/ES (njen peti odstavek 16. člena). Hkrati pojasnjujemo, da se skladno z Direktivo 2016/1148/ES PDS ne sme nalagati nobenih dodatnih priglasitev, zato so bile dodatne varnostne zahteve za PDS iz tega predloga zakona črtane;

- glede pripomb ZB k 9. členu navajamo (sedaj 14. člen tega predloga zakona), da določba ni

povezana z obveznostmi IBS, kar bi člane ZB neposredno zadevalo. Gre za PDS. Elementi, ki se upoštevajo, so skladni z Direktivo 2016/1148/ES. Geografsko območje načeloma ni določeno, treba je namreč upoštevati čezmejni vpliv;

- glede pripomb SOEK k 9. členu pojasnjujemo, da smo z vidika jasnosti člen dopolnili in temu ustrezno tudi obrazložitve;

- pripombe BS k 11.členu so bile v največji možni meri upoštevane;

- pripombe posameznika SŠ k 11. členu, kaj podrobneje mora vsebovati varnostna dokumentacija je bila upoštevana na način, da je v tretjem odstavku sedaj 12. in 17. člena predviden pravilnik, ki bo podrobneje določil vsebino in strukturo varnostne dokumentacije itd.;

- na pripombe k 12. členu, ki so jih podali ICS, ZSČ, IP, MICROSOFT, BS, ZB ter posameznika MK in TV, odgovarjamo, da predlog zakona sedaj loči obveznosti glede zagotavljanja informacijske varnosti (tako glede varnostnih zahtev, varnostne dokumentacije in varnostnih ukrepov ter priglasitve incidentov) s strani zavezancev tega zakona glede na njihovo kategorijo. III. Poglavje tako opredeljuje informacijsko varnost IBS, IV. Poglavje informacijsko varnost PDS in V. Poglavje informacijsko varnost državnih organov (gre za člene od 11 do vključno 18), s katerim se je tako zadostilo določbam Direktive 2016/1148/ES ter nekaterim nacionalnim specifikam (obveznosti državnim organov), ob tem pa so bile tudi upoštevane nekatere pripombe navedenih deležnikov;

- pripombe ZČS k 12. členu naj se izloči seznam minimalnih varnostnih ukrepov pri zavezancih in se nadomesti z obveznosti PNO-ja za pripravo seznama obveznih varnostnih ukrepov niso bile upoštevane, ker PNO nima pristojnosti za izdajo zavezujočih aktov (je pa predviden pravilnik v tretjem odstavku 12. in 17. člena). Glede ohranjanja dnevniških zapisov je ozemlje ohranjanja ter rok ohranjanja le- teh določen v petem odstavku 12. člena (kjer je ugodeno pripombi BS) ter 17. člena. Hkrati pojasnjujemo, da roka glede hrambe dnevniških zapisov PNO ne more spreminjati;

- glede pripomb ZB k 12. člena glede ohranjanja dnevniških zapisov se sklicujemo na prejšnjo alinejo, prav tako glede pripomb TV glede te tematike;

- pripombe MK k 12. členu, da bi v kritični infrastrukturi moralo biti pravilo, da mora ponudnik kupljene opreme zagotavljati brezplačne varnostne popravke (brezplačne zato, ker so njegova napaka in »de facto« napaka v prodanem izdelku) za celotno predvideno obdobje uporabe izdelka, niso bile upoštevane iz razloga, ker je to stvar pogodbenega urejanja (oziroma morebitnega javnega naročanja);

- na pripombe posameznika TV ter ICS k 13. členu pojasnjujemo, da člena v tej vsebini, kot je bil predviden v javni obravnavi (13. člen- ukrepi PNO), sedanji predlog zakona ne vsebuje. Ukrepi PNO-ja v primeru incidenta ali v primeru stanja povišane ogroženosti so sedaj opredeljeni v 21. in 22. členu tega predloga zakona;

- na pripombe ICS k 13. členu glede obveščanja NCKU, in ne Sekretariata Sveta za nacionalno varnost, odgovarjamo, da je v 21. in 22. členu (pri obeh tretji odstavek) tega predloga zakona predvideno obveščanje vlade in Sveta za nacionalno varnost (SNAV), kar je bilo na strokovni ravni ocenjeno kot smiselno;

- pripombe SOEK in posameznika TV k 16. členu so bile upoštevane na način, da smo glede na različne posledice, ki jih ima lahko dotični incident na različnih področjih v določenem časovnem obdobju, časovni kriterij črtali;

- pripombe posameznika TV k 18. členu glede vsebovanja kibernetske obrambe ter s tem povezanih izrazov v zakonu, ni bila upoštevana. Ocenjeno je bilo, da je kibernetsko obrambo (je celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju) z vidika javne varnosti potrebno obdržati;

- pripomba ZČS, ARNES, ZB in posameznika TV k 19. členu glede *a priori* opredelitve vseh podatkov, ki ji vsebujejo seznami, za tajne je bila upoštevana na način, da se le tisti podatki obravnavajo v skladu s predpisi, ki urejajo tajne podatke in poslovno skrivnost, ki so kot taki bili že določeni (ne gre torej za avtomatičnost obravnave vseh podatkov kot tajnih);

- pripombe posameznika NN k 19. členu glede vodenja podatkov o naslovu prebivališča kontaktne osebe v seznamu kot nesorazmernega ukrepa smo upoštevali;

- pripombe TV k 19. členu, da naj se zamenja »kibernetski napad« s »kibernetski incident« (definicija kibernetskega napada pa v 4. členu izpusti) ni bila upoštevana, saj je bilo ocenjeno, da je z vidika zagotavljanja informacijske varnosti obstoj tega termina potreben;

- glede pripombe posameznika TV k 20. členu (sedaj 26. člen) naj se strategija pregleduje pogosteje kot vsakih 5 let, pojasnjujemo, da zakonsko nalaganje obveznosti pregleda le- te ni smotrno, saj mora PNO, v katerega delokrog spada glede na 10. tč. drugega odstavka 27. člena predloga zakona skrb za pripravo in izvajanje strategije, to izvajati po uradni dolžnosti;

- pripombe ICS k 21. členu je bila upoštevana na način, da smo črtali besedo »koordinira« (glej 8. tč. drugega odstavka 27. člena predloga zakona);

- pripombe posameznika TV k 23. členu k izboljšanju jasnosti so bile v največji možni meri upoštevane;

- pripombe AGEN RS k 24. členu je bila upoštevana na način (sedaj 30. člen), da lahko IBS v sodelovanju in s soglasjem pristojnih organov na njihovem področju (npr. regulatorja posameznega področja) vzpostavijo področni SOC. Ta pogoj je bil dodan z vidika izogibanja povzročitve stroškov, ki bi se prevalili na naročnike preko omrežnine;

- pripomba posameznika TV k 25. členu je bila upoštevana na način, da je v sedaj 27. členu (tč. 13 njegovega drugega odstavka) navedeno, da je PNO enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic ter z mrežo skupin CSIRT in s skupino za sodelovanje;

- splošne pripombe ZSČ k X. Poglavju, naj se dodatno opredelijo nosilci kontrole skladnosti z zakonom pri zavezancih ter opredeli organ, ki bo določil metodologijo ugotavljanja, ter da naj PNO - ju zakonodajalec v 21. členu naloži tudi ustrezno pristojnost oblikovanja metodologije nadzora, ki se izvaja pri zavezancih ali pa naj se vsebinsko opredeli kot dodaten člen, niso bile upoštevane. Pri nadzoru se uporablja Zakon o inšpekcijskem nadzoru- ZIN (inšpektor je pristojen za vse ukrepe po njem), poleg teh pa lahko inšpektor odredi še ukrepe, ki so določeni v predlogu zakona. V ZIN je po

našem mnenju dovolj podrobno opisano ravnanje inšpektorjev, specifike nadzora nad IBS, PDS in državnimi organi pa so opisane v treh ločenih členih predloga zakona, dodatno pa je poseben ukrep določen še v 36. členu predloga zakona;

- na splošne pripombe BS k X. Poglavju pojasnjujemo, da sedaj 32. člen predloga zakona določa, da nadzor na zakonom, na njegovi podlagi sprejetih predpisov ter izdanih upravnih odločb, opravljajo inšpektorji za informacijsko varnost v okviru novoustanovljenega PNO. Nadzor nad upoštevanjem navedenih aktov bo torej izvajal ta inšpektor, kar pa ne izključuje nadzora s strani drugih nadzornih organov na podlagi drugih področnih predpisov. Pripombo, naj se predlog zakona sklicuje na sodelovanje nacionalnega organa in pristojnega CSIRT z nadzornim organom za varstvo osebnih podatkov in ne z Informacijskim pooblaščencem, ni bila upoštevana, saj je v zakonskem besedilo potrebno ta organ z vidika jasnosti in pravne varnosti konkretizirati;

- pripombe posameznika BK k 27. členu (glede tega tudi posameznik TV), naj se uporablja termin »aktivni preizkušeni revizor informacijskih sistemov« nismo upoštevali, ker je ta termin preozek, prav tako pa je termin »kvalificirani revizor« bolj tehnološko nevtralen;

- pripombo PLINOVODI k 29. členu smo upoštevali v 36. členu (posebni ukrep) predloga zakona;

- pripombe ZB k 31. členu (prekrškovne določbe so sedaj za vsako kategorijo zavezancev določene ločeno- 38., 39. in 40. člen) za znižanje globe ni bila upoštevana, saj smo ocenili, da bodo predvidene predpisane kazni učinkovite, sorazmerne in odvračalne, kar zahteva 21. člen Direktive 2016/1148/ES;

- na pripombe ICS k 32. členu glede rokov za pričetek delovanja PNO odgovarjamo, da je po naši oceni sedaj postavljen rok (sedaj v 41. členu) izvedljiv, v vladnem gradivu so navedeni tudi resursi, ki bodo dani za ta namen. SI CERT bo izvajal naloge nacionalnega CSIRT. Glede pripomb o razmerju PNO in UVTP pojasnjujemo, da v predlogu predviden 41. člen ureja začetek delovanja PNO (predvidoma tako imenovana »Uprava RS za informacijsko varnost«), ki začne z delovanjem najkasneje do dne 1. januarja 2020. S tem dnem 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. Do pričetka delovanja PNO njegove naloge opravlja UVTP skladno s tem zakonom, razen nalog upravnega odločanja in nadzora, ki jih opravlja ministrstvo, pristojno za informacijsko družbo. Namreč, UVTP kot vladna služba sistemsko ne more izvajati nalog upravnega odločanja in nadzora. Zaradi odložitve pričetka delovanja PNO je potrebno zagotoviti, da se bo ZIV izvajal pred 1. januarjem 2020 v polnem obsegu in skladno z direktivo, ki se prenaša.

- pripombe ARNES k 33. členu so bile upoštevane.

Za deležnike so potekale tudi javne predstavitve v osnutku ZIV predvidenih rešitev (kot je bil le-ta dan v javno obravnavo), in sicer:

- 14. septembra 2017 v Ljubljani na Posvetu o prepletanju aktualne zakonodaje glede kibernetske varnosti in poročanja o incidentih;
- 6. oktobra 2017 na Direktoratu za informacijsko družbo, MJU, predstavnikom SOS;

- 8. novembra 2017 na konferenci Informacijska varnost na Institutu Jožef Stefan ter pri sodelovanju na okrogli mizi.

8. PODATEK O ZUNANJEM STROKOVNJAKU OZIROMA PRAVNI OSEBI, KI JE SODELOVALA PRI PRIPRAVI PREDLOGA ZAKONA, IN ZNESKU PLAČILA ZA TA NAMEN

Pri pripravi predloga zakona niso sodelovali zunanji strokovnjaki oziroma pravne osebe.

9. NAVEDBA, KATERI PREDSTAVNIKI PREDLAGATELJA BODO SODELOVALI PRI DELU DRŽAVNEGA ZBORA IN DELOVNIH TELES

- Boris Koprivnikar, minister, Ministrstvo za javno upravo,
- mag. Ksenija Klampfer, državna sekretarka, Ministrstvo za javno upravo,
- dr. Nejc Brezovar, državni sekretar, Ministrstvo za javno upravo,
- mag. Bojan Križ, generalni direktor, Direktorat za informacijsko družbo, Ministrstvo za javno upravo,
- Barbara Pernuš Grošelj, sekretarka, Direktorat za informacijsko družbo, Ministrstvo za javno upravo.

II. BESEDILO ČLENOV

Zakon o informacijski varnosti

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 (v nadaljnjem besedilu: RS), ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti 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 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 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 (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 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 ponudnika storitev sistema domenskih imen najvišje ravni.
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 6. 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 informacijski sistemi so vsi informacijski sistemi subjekta, brez katerih ni mogoče

neprekinjeno izvajati storitev.

15. Krmilni informacijski sistemi so informacijski sistemi, ki omogočajo izvajanje pravilnih postopkov in izvajajo ustrezno sosledje delovanja ključnih informacijskih sistemov subjekta.
16. Mreža skupin CSIRT je povezava, v kateri sodelujejo skupine CSIRT iz držav članic in CERT-EU.
17. Nadzorni informacijski sistemi so informacijski sistemi, ki skrbijo za izvajanje nadzorstvene funkcije informacijskih sistemov subjekta.
18. Obvladovanje incidentov so vsi postopki, ki omogočajo odkrivanje, analizo in zajezitev incidentov ter odzivanje nanje.
19. 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 le-teh 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.
20. Ponudnik digitalnih storitev je vsaka fizična ali pravna oseba, ki zagotavlja digitalno storitev.
21. Ponudnik storitev sistema domenskih imen je subjekt, ki zagotavlja storitve sistema domenskih imen na internetu.
22. 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.
23. Register domenskih imen najvišje ravni je 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 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.
25. Sistem domenskih imen je 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. SOC je varnostno operativni center, ki se odziva na incidente na področju informacijske

varnosti.

28. Specifikacija je dokument, ki predpisuje tehnične zahteve, ki jih mora izpolniti proizvod, proces, storitev ali sistem.
29. 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.
30. 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.
31. Standard je tehnična specifikacija, ki jo je sprejel priznan organ za standardizacijo za večkratno ali stalno uporabo.
32. 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.
33. 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).
34. Storitev računalništva v oblaku je digitalna storitev, ki omogoča dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov.
35. 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 RS.
36. Tveganje je vsako razumno določljivo okoliščino ali dogodek, ki ima lahko negativen učinek na varnost omrežij in informacijskih sistemov.
37. 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.

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 RS (v nadaljnjem besedilu: vlada) določi seznam bistvenih storitev iz Uredbe o standardni klasifikaciji dejavnosti (Uradni list RS, št. 69/07 in 17/08).

(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 RS in še kateri drugi državi članici EU, se pristojni nacionalni organ pred določitvijo izvajalcev bistvenih storitev iz drugega odstavka ali prejšnjega odstavka tega člena posvetuje s pristojnim nacionalnim organom države članice EU, kjer izvajalec takšne storitve zagotavlja.

7. 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 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 upoštevajo tudi področni dejavniki.

(4) Področne dejavnike iz prejšnjega odstavka in metodologijo za določitev izvajalcev bistvenih storitev določi vlada.

8. člen

(določitev ponudnikov digitalnih storitev)

(1) Ponudniki digitalnih storitev iz druge alineje prvega odstavka 5. člena tega zakona izpolnjujejo obveznosti po tem zakonu neposredno.

(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)

Vlada določi organe državne uprave iz tretje alineje prvega odstavka 5. člena tega zakona in CSIRT organov državne uprave, v kolikor organi državne uprave nimajo zagotovljenih lastnih zmogljivosti vsaj na ravni SOC.

10. člen

(določitev kontaktne osebe zavezancev)

(1) Izvajalci bistvenih storitev določijo in pooblastijo kontaktno osebo za informacijsko varnost in njenega namestnika ter kontaktne podatke posredujejo pristojnemu nacionalnemu organu v 15 dneh od določitve vlade iz drugega odstavka 6. člena tega zakona.

(2) Organi državne uprave lahko določijo in pooblastijo kontaktno osebo za informacijsko varnost in

njenega namestnika ter te kontaktne podatke posredujejo pristojnemu nacionalnemu organu.

(3) Ponudnik digitalnih storitev, ki ima skladno s prvim odstavkom 15. člena tega zakona glavni sedež v RS, 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 Evropski uniji (v nadaljnjem besedilu: EU), vendar določi sedež svojega predstavnika za EU v RS 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 četrtega odstavka 7. 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 upravljanja le-tega;
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) določi vsebino in strukturo varnostne dokumentacije ter metodologijo izvedbe analize obvladovanja tveganj iz prvega odstavka tega člena in minimalen obseg in vsebino varnostnih ukrepov iz prejšnjega 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 lahko dopolni skladno s tem zakonom.

(5) Izvajalci bistvenih storitev za namen obvladovanja incidentov, skladno z analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj, ki jo izvedejo po metodologiji iz četrtega odstavka 7. člena tega zakona, ob upoštevanju stanja tehnike zagotovijo tudi ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja, vendar ne manj kot šest mesecev. Ohranjanje teh dnevniških zapisov se zagotavlja na ozemlju RS, razen za področja digitalna infrastruktura, bančništvo in infrastruktura finančnega trga, pri katerih se to 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 RS, 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) Posredovanje informacij in podatkov iz prejšnjega odstavka, ki so zaupni, je omejeno na obseg,

ki je ustrezen in sorazmeren glede na namen te izmenjave.

(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 ustrezne 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 zgoraj navedene parametre.

(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 RS, 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 ali nacionalni CSIRT obvestita druge prizadete države članice EU, če incident zadeva dve ali več držav članic EU ali v drugih primerih, če ocenita, 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) 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 ponudnikov digitalnih storitev, ki priglasijo incidente, na drugi strani.

15. člen

(pristojnost in teritorialnost)

(1) Ponudnik digitalnih storitev, ki ima glavni sedež v RS, 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 RS, če ima v RS 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 RS, 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 RS, 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, 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.

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

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 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 ustrezne 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 upravljanja le-tega,
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 ter metodologijo

izvedbe analize obvladovanja tveganj iz prvega odstavka tega člena in minimalen obseg ter vsebino varnostnih ukrepov iz prejšnjega 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 lahko 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, vendar ne manj kot šest mesecev. Ohranjanje teh dnevniških zapisov mora biti zagotovljeno na ozemlju RS.

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 SOC, 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 RS, 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 spodbuja uporabo evropskih ali mednarodno sprejetih standardov in specifikacij, pomembnih za varnost omrežij in informacijskih sistemov in v ta namen ustrezne 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, po potrebi v sodelovanju s pristojnim nacionalnim organom. 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 ustrezne 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 ustrezne 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 širše javnosti, pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, pripravi ustrezno sporočilo (v nadaljnjem besedilu: splošno opozorilo) 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, v katere lahko skladno s svojimi pristojnostmi vključijo družbene potenciale, potrebne za zagotavljanje celovite informacijske varnosti.

(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 le-teh 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 osnovni okvir za izvedbo ukrepov, ki bodo pripomogli k vzpostavitvi učinkovitega nacionalnega sistema zagotavljanja informacijske varnosti. S tem namenom opredeljuje strateške cilje ter ustrezne 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 deležnikov, 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, s področnimi varnostno-operativnimi centri, če ti obstajajo, z regulatorji oziroma nadzorniki področij iz drugega odstavka 5. člena, z Agencijo za komunikacijska omrežja in storitve RS, 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. za namene pregleda Direktive 2016/1148/ES, ki ga izvede EK, le-to redno oziroma 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;
13. 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;
14. izpolnjuje druge obveznosti obveščanja EK in skupine za sodelovanje, obveznosti obveščanja in notifikacije preostalih mednarodnih organizacij;
15. 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 po potrebi objavlja opozorila;
3. sodeluje v mreži skupin CSIRT;
4. sodeluje s skupinami CSIRT in varnostno-operativnimi centri v RS 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.

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

(SOC)

(1) Izvajalci bistvenih storitev iz posameznega področja, navedenega v drugem odstavku 5. člena tega zakona, lahko v sodelovanju in s soglasjem pristojnih organov za to področje vzpostavijo področni SOC, če ocenijo, da je na posameznem področju to potrebno. Področni SOC pomaga izvajalcem bistvenih storitev pri odzivanju na incidente. Pri tem sodeluje z nacionalnim CSIRT in pristojnim nacionalnim organom.

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

(3) Organi državne uprave lahko na svojem področju dela vzpostavijo SOC, če ocenijo, da je na posameznem področju to potrebno. SOC pomaga organom državne uprave pri odzivanju na incidente. Pri tem sodeluje s pristojnim nacionalnim organom.

31. člen

(sodelovanje na nacionalni ravni)

(1) Pristojni nacionalni organ in nacionalni CSIRT ter CSIRT organov državne uprave sodelujejo pri izpolnjevanju obveznosti. Pri tem nacionalni CSIRT in CSIRT organov državne uprave svojo dejavnost usklajujeta s pristojnim nacionalnim organom in drugimi pristojnimi organi.

(2) Nacionalni CSIRT in CSIRT organov državne uprave pristojnemu nacionalnemu organu štirikrat letno posredujeta poročilo o izvajanju svojih nalog.

(3) 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

32. 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 pri obravnavi zadev iz prvega odstavka tega člena, katerih posledica je kršitev varstva osebnih podatkov, sodeluje z Informacijskim pooblaščencem. Za namen pravočasnega ukrepanja v smeri zagotavljanja odprave kršitev Informacijskega pooblaščenca obvešča tudi v primerih suma kršitve varstva osebnih podatkov.

(4) Tožba v upravnem sporu zoper dokončno odločbo, izdano v postopkih nadzora iz prejšnjega odstavka, se vloži na sedežu Upravnega sodišča RS. Postopek je nujen in prednosten.

33. člen

(nadzor nad izvajalci bistvenih storitev)

(1) Inšpektor nadzira, ali izvajalci bistvenih storitev izpolnjujejo njihove 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 s tem povezane posledice 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.

34. 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 njihove 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) Izmenjava informacij in podatkov iz prejšnjega odstavka, ki so zaupni, je omejena na obseg, ki je ustrezen in sorazmeren glede na namen te izmenjave.

35. člen

(nadzor nad organi državne uprave)

(1) Inšpektor nadzira, ali organi državne uprave izpolnjujejo njihove 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 s tem povezane posledice 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.

36. člen

(posebni ukrep)

Ne glede na določbe zakona, ki ureja inšpekcijski nadzor, lahko inšpektor zavezancem le v skrajnem primeru in upoštevaje področni pomen sistema ter njihovo dejavnost prepove uporabo tega sistema ali njegovega dela, dokler ni ugotovljena pomanjkljivost odpravljena in če s tem ukrepom ni ogrožena zanesljivost oskrbe v posameznem sistemu.

XI. Kazenske določbe

37. 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.

38. 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.

39. 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.

40. 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

41. 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.

42. člen

(delovanje drugih pristojnih organov)

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

(2) Nacionalni CSIRT mora v roku iz prejšnjega odstavka izpolniti zahteve iz Priloge 1 Direktive 2016/1148/ES.

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

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

43. 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, do sprejetja katere se uporablja Strategija kibernetske varnosti Republike Slovenije, ki jo je sprejela vlada dne 25. februarja 2016 s sklepom št. 38100-12/2015/5.

44. 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 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 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 skladno s tem zakonom v dvanajstih mesecih od njihove določitve iz prejšnjega odstavka.

XIII. Končna določba

45. člen

(začetek veljavnosti)

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

III. OBRAZLOŽITEV

1. Splošne določbe

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

K 1. členu

Predlog člena opredeljuje vsebino zakona, ki predstavlja prvo sistemsko osnovo za celovito ureditev informacijske varnosti na določenih ključnih področjih v Republiki Sloveniji (v nadaljnjem besedilu: RS).

Predlog zakona ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v RS, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti 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 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.

K 2. členu

Predlog člena v prvem odstavku najprej pojasnjuje namen predloga zakona, ki je ureditev področja informacijske varnosti in 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.

S tem zakonom se v pravni red prenaša Direktiva 2016/1148/ES, kot navaja predlagan drugi odstavek. Direktiva v Uvodni izjavi št. 6 določa, da je za učinkovito odzivanje na izzive na področju varnosti omrežij in informacijskih sistemov potreben globalni pristop na ravni Evropske unije (v nadaljnjem besedilu: EU), ki bo obsegal skupne minimalne zahteve za vzpostavitev in načrtovanje zmogljivosti, izmenjavo informacij ter sodelovanje in skupne varnostne zahteve za izvajalce bistvenih storitev (v nadaljnjem besedilu: IBS) in ponudnike digitalnih storitev (v nadaljnjem besedilu: PDS). Vendar IBS in PDS nič ne preprečuje, da sami izvajajo varnostne ukrepe, ki so strožji od tistih, določenih v tej direktivi. Poleg prenosa Direktive 2016/1148/ES se s predlogom zakona, oziroma z njegovimi nacionalnimi določbami ureja varnost omrežij in informacijskih storitev v nekaterih organih državne uprave.

V tretjem odstavku se sledi določbi tretjega odstavka 1. člena Direktive 2016/1148/ES ter njeni Uvodni izjavi št. 7, ki določa, da se obveznosti IBS in PDS ne bi smele uporabljati za podjetja, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve v smislu Direktive EU 2002/21/ES, za katera veljajo posebne zahteve glede varnosti in celovitosti, določene v navedeni direktivi, katere določbe (konkretno člena 13a in 13b) so v RS prenesene v zakon, ki ureja elektronske komunikacije (Zakon o elektronskih komunikacijah, Uradni list RS, št. št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17; v nadaljnjem besedilu: ZEKom-1), konkretno v njegovo VII. poglavje. V tem poglavju je določeno, da morajo operaterji sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev ter tudi za zagotovitev celovitosti svojih omrežij, zlasti zaradi preprečevanja in zmanjševanja učinkov varnostnih incidentov na uporabnike in medsebojno

povezana omrežja. Sprejeti ukrepi morajo ob upoštevanju stanja zagotoviti raven varnosti, primerno predvidenemu tveganju. Med ukrepe spadata tudi sprejem in izvajanje ustreznega varnostnega načrta, ki ga operater določi kot poslovno skrivnost. Določeni sta tudi obveznost poročanja o kršitvah varnosti ali celovitosti Agenciji za komunikacijska omrežja in storitve (v nadaljnjem besedilu: AKOS) ter obveznost privolitve operaterjev v revizijo varnosti.

Določbe se skladno z zgoraj navedenimi določbami Direktive 2016/1148/ES in uvodno izjavo prav tako ne bi smele uporabljati za ponudnike storitev zaupanja v smislu Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta, za katere veljajo varnostne zahteve iz navedene uredbe, kar je določeno v tretjem odstavku 2. člena predloga zakona.

K 3. členu

S predlogom člena se prenaša določba 2. člena Direktive 2016/1148/ES, ki zahteva, da se obdelava osebnih podatkov na podlagi te direktive (torej vključno z nacionalnimi zakoni, ki jo prenašajo) izvaja v skladu s predpisi EU, ki urejajo varstvo osebnih podatkov.

Zato je predlagano, da se obdelava osebnih podatkov na podlagi tega zakona izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov.

Z vidika varstva zaupnosti podatkov in informacij, ki se obdelujejo na podlagi tega predloga zakona in so opredeljeni kot tajni ali kot poslovna skrivnost, je v tem členu še predlagano, da se le-ti obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost.

K 4. členu

V predlogu člena se pojasnjujejo uporabljeni izrazi; opredelitve izrazov so večinoma povzete po Direktivi 2016/1148/ES (njen 4. člen), v delu, ko gre za nacionalne določbe, pa po opredelitvah strokovnih pojmov s področja informacijske varnosti oziroma obramboslovja.

2. Zavezanci

V tem poglavju so navedeni zavezanci po predlogu tega zakona, opredeljena so merila in metodologija za določitev IBS, PDS in organov 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), ter določitev kontaktne osebe zavezancev.

K 5. členu

V predlogu člena se določajo zavezanci za obveznosti, ki se nanašajo na varnostne zahteve in na priglasitve incidentov iz predloga zakona. Poleg zavezancev, ki izhajajo iz Direktive 2016/1148/ES, torej IBS in PDS (ki so ponudniki spletnih tržnic, računalništva v oblaku in spletnih iskalnikov kot jih za namene 5. točke 4. člena Direktive 2016/1148/ES določa njena Priloga III), se v okviru nacionalne določbe kot zavezanci določijo tudi organi državne uprave. Za slednje veljajo podobne obveznosti kot za IBS, ampak v prilagojeni obliki ter z nekaterimi izjemami. Ob tem še pojasnjujemo, da predlog tega zakona ne posega v centralizacijo državne informatike. Organe državne uprave, ki bodo zavezanci, bo določila vlada na podlagi 9. člena predloga tega zakona. Ob tem bo seveda upoštevala tudi dejansko stanje na področju centralizacije informatike. V primeru, ko je skrbnik oziroma upravljavec informacijskih sistemov in omrežij ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave (sedaj Ministrstvo za javno upravo - MJU), bo le-to tudi pristojno in odgovorno za izvajanje varnostnih ukrepov. V kolikor pa obstajajo primeri, ko so oziroma bodo informacijski sistemi in omrežja v upravljanju posameznih drugih organov državne uprave oziroma bodo le-ti izvajali informacijske storitve, bodo ti organi s sklepom vlade določeni kot zavezanci po predlogu tega zakona in bodo posledično tudi poskrbeli za

izvajanje varnostnih ukrepov v okviru svojih pristojnosti. Popolne centralizacije informatike verjetno nikoli ne bo, je pa res, da bo zaradi nje veliko manj zavezancev, ker bo to vlogo v večini primerov prevzel MJU.

Hkrati predlog člena v drugem odstavku opredeljuje področja na katerih delujejo IBS, kot jih za namene 4. točke 4. člena Direktive 2016/1148/ES določa njena Priloga II. Poleg sedmih področij iz te priloge direktive (to so energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura finančnega trga), ki so po direktivi obvezni, se v predlogu tega člena dodata, kot nacionalna določba, še dve področji (preskrba s hrano in varstvo okolja), ki sta kot pomembni področji prepoznani tudi v sorodnem zakonu, ki ureja kritično infrastrukturo, s čimer se v tem delu ta predlog zakona približuje navedenemu zakonu.

K 6. členu

Z namenom prenosa 5. člena Direktive 2016/1148/ES se v predlogu člena uredi režim določitve IBS. Predlagano je, da Vlada RS (v nadaljnjem besedilu: vlada) z uredbo najprej določi seznam bistvenih storitev iz Uredbe o standardni klasifikaciji dejavnosti (Uradni list RS, št. 69/07 in 17/08) torej v obrazložitvi k 5. členu navedenih obveznih sedmih področjih iz Direktive 2016/1148/ES ter dveh dodatnih: preskrba s hrano in varstvo okolja), ki se štejejo za bistvene za potrebe tega zakona (opredelitev bistvene storitve je vsebovana v 1. tč. 4. člena predloga zakona; in sicer je »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«).

Nadalje je v predlaganem drugem odstavku določeno, da vlada na podlagi meril iz 7. člena tega predloga zakona (v katerem gre za prenos drugega odstavka 5. člena Direktive 2016/1148/ES, kjer so določena merila za določitev IBS) določi posameznega IBS.

Tretji odstavek določa, da so ne glede na določbo drugega odstavka tega člena (torej ne glede na merila iz njegovega 7. člena) vlada kot IBS določi tudi tisti upravljavce kritične infrastrukture, določene v skladu s predpisi, ki urejajo področje kritične infrastrukture, in nosilce obrambnega načrtovanja, določene v skladu s predpisi, ki urejajo področje obrambe, katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov. Določba je torej omejena na tiste določene upravljavce kritične infrastrukture in nosilce obrambnega načrtovanja, ki so sploh povezani s področjem urejanja tega zakona, namreč, informacijsko varnostjo, kar predpostavlja njihovo odvisnost od omrežij in informacijskih sistemov. Brez te omejitve bi bila namreč določba za nekatere zavezance lahko brezpredmetna. Pri tem pa je potrebno poudariti, da predlog zakona v tretjem odstavku 2. člena izključuje svojo uporabo za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve, kar velja torej tudi pri izvajanju tretjega odstavka 6. člena, saj njegova uporaba ni bila izključena. Glej tudi obrazložitev k 2. členu.

Če izvajalec zagotavlja bistveno storitev v RS in še kateri drugi državi članici EU, se pristojni nacionalni organ pred določitvijo izvajalcev bistvenih storitev iz drugega odstavka ali prejšnjega odstavka tega člena posvetuje s pristojnim nacionalnim organom države članice EU, kjer izvajalec takšne storitve zagotavlja.

K 7. členu

V tem členu so za potrebe 6. člena (glej tudi prejšnjo obrazložitev) tega predloga zakona (določitev IBS) podrobneje opredeljena merila, ki se upoštevajo pri določitvi IBS, kot jih opredeljuje drugi odstavek 5. člena Direktive 2016/1148/ES. Glede na navedeno gre za subjekt, ki zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih oziroma gospodarskih dejavnosti; zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov, incident pa bi imel pomemben negativen vpliv na zagotavljanje te storitve (opredelitev bistvene storitve je vsebovana v 1. tč. 4. člena predloga zakona; in sicer je »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«).
Skladno s četrtim odstavkom tega člena bo metodologijo za določitev IBS ter področne dejavnike, ki se upoštevajo pri odločanju, ali bi incident imel pomemben negativen vpliv, vlada predpisala v uredbi. Da bo uredba čimbolj skladna s pristopom držav članic EU, bo v pomoč tudi podpora skupine za sodelovanje (npr. priporočila skupine za usklajevanje za usklajen pristop za določitev IBS v EU).

K 8. členu

V tem členu so določeni PDS, ki so zavezanci na podlagi predloga zakona. Pri tem je treba hkrati upoštevati 4. točko (v povezavi s 33. točko) 4. člena predloga zakona, ki opredeljuje »digitalno storitev«. Le-ta za potrebe tega zakona pomeni naslednje storitve informacijske družbe: storitve spletne tržnice, spletnega iskalnika in računalništva v oblaku (podrobneje opredeljene v 29., 30. in 34. točki 4. člena predloga zakona). Kot zavezanci so izvzeti tisti PDS, ki so pripoznani kot majhna (kar vključuje tudi mikro) podjetja, kot je to opredeljeno v predlaganem drugem odstavku (kot to določa enajsti odstavek 16. člena Direktive 2016/1148/ES, ki se sklicuje na Priporočila EK 2003/361/ES).

K 9. členu

Ker so v okviru nacionalne določbe kot zavezanci tega predloga zakona določeni tudi organi državne uprave, se v tem členu opredeljuje režim določitve le-teh. Predlagano je, da jih določi vlada s sklepom kot tudi CSIRT organov državne uprave, v kolikor organi državne uprave nimajo zagotovljenih lastnih zmogljivosti vsaj na ravni varnostno-operativnega centra (v nadaljnjem besedilu: SOC (v angleščini »Security Operating Center«)). Ob tem se sklicujemo tudi na že podano obrazložitev k 5. členu v delu, ki se nanaša na organe državne uprave.

K 10. členu

Ta člen vsebuje določbe o obveznosti določitve kontaktne osebe (in njenega namestnika) zavezancev ter o posredovanju njenih podatkov PNO. Gre za nacionalno določbo.
Pri tem se prvi odstavek nanaša na IBS, ki morajo posredovati navedene podatke.
Za razliko od IBS pa organi državne uprave ter PDS niso obvezani k določitvi kontaktne osebe, ampak jima je dana zgolj možnost, da dotične podatke PNO-ju posredujeta, kar določajo drugi, tretji in četrti odstavek.
Peti odstavek pa vzpostavlja obveznost poročanja IBS v primeru morebitne spremembe kontaktnih podatkov.

3. Informacijska varnost IBS

V predlaganem poglavju se vzpostavljajo obveznosti IBS glede varnostnih zahtev, varnostne dokumentacije, varnostnih ukrepov in priglasitve incidentov, kot zahtevajo določbe IV. poglavja Direktive 2016/1148/ES. Direktiva določbe o informacijski varnosti IBS ter PDS vsebuje ločeno, kar je skladno z njeno Uvodno izjavo št. 57. Ta izjava navaja, da se zaradi temeljnih razlik med IBS, zlasti glede njihove neposredne povezanosti s fizično infrastrukturo, in PDS, zlasti glede njihove čezmejne narave, v predlogu zakona sprejme ločen pristop k ravni harmonizacije za obe skupini subjektov. Kar zadeva varnostne zahteve in zahteve glede priglasitve, ta zakon zagotavlja visoko stopnjo harmonizacije tudi za PDS. Enako bodo zagotavljali izvedbeni akti, ki bodo sprejeti na njegovi podlagi. To omogoča enotno obravnavo PDS v EU, sorazmerno z njihovo naravo in stopnjo tveganja, ki bi mu lahko bili izpostavljeni.

K 11. členu

Predlagan člen sledi zahtevam prvega in drugega odstavka 14. člena Direktive 2016/1148/ES ter opredeljuje obveznost IBS, da določijo svoje ključne, krmilne in nadzorne informacijske sisteme ter

dele omrežja, s katerimi zagotavljajo izvajanje bistvenih storitev. Prav tako morajo izvesti analizo, oceno in vrednotenje tveganj ter na tej podlagi pripraviti in izvesti ukrepe, potrebne za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri bistvenih storitvah.
Skladno s tretjim odstavkom morajo IBS sprejeti ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov na varnost tistih omrežij in informacijskih sistemov, ki se uporabljajo za zagotavljanje bistvenih storitev, da bi zagotovili neprekinjeno izvajanje teh storitev, kot določa drugi odstavek 14. člena Direktive 2016/1148/ES.
Skladno s četrtim odstavkom IBS, ki 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.

K 12. členu

S predlogom člena, pri katerem ne gre za prenos Direktive 2016/1148/ES, so predvidene glavne varnostne zahteve za IBS, vključno s predvideno varnostno dokumentacijo, na podlagi katere morajo IBS pripraviti in izvajati potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe; vsebino bo podrobneje uredil pravilnik (kot je to določeno v predlaganem tretjem odstavku).
Z opredelitvijo varnostne dokumentacije se pri IBS doseže bolj poenoten pristop k izdelavi te dokumentacije in se jih s tem, brez omembe standarda, vsebinsko napotuje na uveljavljene in standardizirane pristope (na primer razred standardov ISO 27000), ki naj jim bodo pomoč pri izdelavi dokumentacije.
Z namenom zmanjševanja administrativnih bremen in zagotavljanja pravne varnosti ter sorazmernosti lahko IBS v primeru upoštevanih varnostnih zahtev iz zakonodaje področij, na katera spadajo, svojo že izdelano varnostno dokumentacijo (le) dopolnijo skladno s tem zakonom, kot to določa predlagani četrti odstavek. IBS zaradi obvladovanja incidentov zagotovijo ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja (ne manj kot šest mesecev) v RS, razen za področja digitalna infrastruktura, bančništvo in infrastruktura finančnega trga, pri katerih se to lahko zagotavlja na ozemlju EU.
Zaradi vrste zgodovinskih, a še vedno delujočih računalnikov ali informacijskih sistemov ali delov omrežij (tako imenovani »legacy« sistemi) se pri izpolnjevanju zavez glede ohranjanja dnevniških zapisov v predlogu tega člena upošteva stanje tehnike. Vse morebitne siceršnje ranljivosti, ki izhajajo iz stanja tehnike, ter zlasti morebitna povečana tveganja je treba upoštevati pri oceni tveganj in pri izdelavi varnostne dokumentacije.

K 13. členu

Predlog člena prenaša določbe 14. člena Direktive 2016/1148/ES o priglasitvah incidentov za IBS (upošteva se tudi določbe Uvodne izjave št. 32). Skladno s to določbo nacionalni CSIRT, ki je skladno s tem predlogom zakona (predlagan 28. člen, glej tudi njegove obrazložitve) odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT (Slovenian Computer Emergency Response Team, v nadaljnjem besedilu: SI CERT) pri javnem zavodu Akademska in raziskovalna mreža Slovenije (v nadaljnjem besedilu: Arnes), prejema priglasitve incidentov, ki jih brez nepotrebnega odlašanja izvedejo IBS. Določeni so tudi režim zavarovanja dnevniški zapisov oziroma revizijskih sledi in postopek ravnanja z zaupnimi podatki ter informacijami, postopek nadaljnjega obveščanja drugih organov (PNO, policije in Nacionalnega centra za krizno upravljanje, v primeru morebitnega čezmejnega vpliva tudi pristojnih organov drugih držav), posredovanje informacij s strani nacionalnega CSIRT ki bi lahko pripomogle k temu, da bi IBS učinkovito obvladal incident, ter postopek v primeru morebitnega obveščanja javnosti.
S tem se upošteva tudi Uvodna izjava št. 32, ki govori o tem, da bi pristojni organi ali skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT) morali prejemati priglasitve incidentov. Enotne kontaktne točke ne bi smele neposredno prejemati priglasitev incidentov, razen če niso istočasno v vlogi pristojnega organa ali skupine CSIRT. Kljub temu bi pristojni organ ali skupina CSIRT morala imeti možnost enotni kontaktni točki naložiti, da priglasitve

incidentov pošlje enotnim kontaktnim točkam drugih držav članic, na katere je incident vplival.

4. Informacijska varnost PDS

Poglavje ureja varnostne zahteve in priglasitev incidentov od PDS ter vsebuje določbe glede pristojnosti in teritorialnosti.

K 14. členu

Predlagan člen prenaša določbe 16. člena Direktive 2016/1148/ES o varnostnih zahtevah ter določbe tretjega, četrtega in petega odstavka 16. člena o priglasitvah incidentov za PDS (ter upošteva tudi Uvodno izjavo št. 32).
Opredeljena je obveznost PDS, da določijo in sprejmejo ustrezne ter sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju storitev v EU. Hkrati morajo sprejeti ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov, na storitve, ki jih ponujajo v EU, da bi zagotovili njihovo neprekinjeno izvajanje, kot določa drugi odstavek 16. člena Direktive 2016/1148/ES.
Tretji odstavek določa, da nacionalni CSIRT prejema priglasitve incidentov (ki imajo pomemben vpliv na zagotavljanje storitev PDS), ki jih brez nepotrebnega odlašanja izvedejo PDS. V členu so določeni tudi režim ravnanja z zaupnimi podatki in informacijami, postopek priglasitve v primeru, kadar je IBS pri zagotavljanju svojih storitev odvisen od tretjega PDS, ter postopek nadaljnjega obveščanja o incidentu drugih organov (PNO, policije in Nacionalnega centra za krizno upravljanje, v primeru morebitnega čezmejnega vpliva tudi pristojnih organov drugih držav) ter postopek v primeru morebitnega obveščanja javnosti.

K 15. členu

Člen prenaša določbe prvega in drugega odstavka 18. člena Direktive 2016/1148/ES ter upošteva njeni Uvodni izjavi št. 64 in št. 65. Predlagana so pravila pristojnosti za PDS, pri čemer so organi v RS pristojni, če ima PDS glavni sedež v RS (glavni sedež je tam, kjer je glavna uprava), kot to določa prvi odstavek.

Drugi odstavek določa, da če PDS, ki nima sedeža v EU, v njej pa zagotavlja takšne storitve, določi sedež svojega predstavnika za EU v RS, kjer tudi zagotavlja digitalne storitve, tudi ta PDS spada v pristojnost organov RS.
Tretji odstavek pa določa ravnanje v primeru nepristojnosti organov RS za PDS; in sicer morajo pristojni organi RS (v primeru, da je delovanje tega PDS kakorkoli povezano z RS) sodelovati s pristojnimi organi drugih držav članic EU, zaradi zagotavljanja medsebojne pomoči, ter si po potrebi izmenjevati informacije na način, kot je potrebno in sorazmerno. 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 četrtem odstavku je tudi določen obseg upravljanja z zaupnimi podatki, gre za prenos petega odstavka 1. člena Direktive 2016/1148/ES.

5. Informacijska varnost organov državne uprave

Poglavje ureja varnostne zahteve, varnostno dokumentacijo in varnostne ukrepe ter priglasitev incidentov, ki jo izvedejo organi državne uprave.

K 16. členu

Pri predlogu tega člena ne gre za prenos določb Direktive 2016/1148/ES, temveč za urejanje nacionalne specifike. Ta člen ureja varnostne zahteve za zavezance, ki so organi državne uprave.

V predlaganem členu je določeno, podobno kot za IBS v 11. členu, da morajo organi državne uprave izvesti analizo, oceno in vrednotenje tveganj ter na tej podlagi pripraviti in izvesti ukrepe, potrebne za obvladovanje tveganj za informacijske sisteme in dele omrežja, s katerimi upravljajo, oziroma za informacijske storitve, ki jih izvajajo in so nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti ter obveznost sprejetja ustreznih ukrepov 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. Prav tako organi državne uprave v primeru, ko 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. Dodatno se ob tem sklicujemo tudi na že podano obrazložitev k 5. členu v delu, ko se ta nanaša na organe državne uprave.

K 17. členu

Določbe tega člena, ki veljajo za organe državne uprave, so podobne in primerljive s tistimi, ki so določene za IBS v 12. členu predloga tega zakona.
Predlog člena za organe državne uprave določa ključne varnostne zahteve, vključno z v zakonu predvideno varnostno dokumentacijo, na podlagi katere le-ti pripravijo in izvajajo potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe, vsebino pa bo podrobneje uredil pravilnik, kot je to določeno v predlaganem tretjem odstavku
Z opredelitvijo varnostne dokumentacije se doseže bolj poenoten pristop pri izdelavi zadevne dokumentacije v organih državne uprave. S tem se jih, brez omembe standarda, vsebinsko napotuje na uveljavljene in standardizirane pristope (na primer razred standardov ISO 27000), ki naj jim bodo v pomoč pri izdelavi dokumentacije.
Z namenom zmanjševanja administrativnih bremen in zagotavljanja pravne varnosti ter sorazmernosti lahko organi državne uprave je v predlaganem četrtem odstavku določeno, da v primeru, da imajo že izdelano varnostno dokumentacijo na podlagi drugih predpisov, le- to lahko (le) dopolnijo skladno s tem zakonom.
Zaradi vrste zgodovinskih, a še vedno delujočih računalnikov ali informacijskih sistemov ali delov omrežij (tako imenovani »legacy« sistemi) se pri izpolnjevanju zavez glede ohranjanja dnevniških zapisov v predlogu tega člena upošteva stanje tehnike. Vse morebitne siceršnje ranljivosti, ki izhajajo iz stanja tehnike, ter zlasti morebitna povečana tveganja je treba upoštevati pri oceni tveganj in pri izdelavi varnostne dokumentacije.
Pri ohranjanju dnevniških zapisov se, drugače kot pri IBS, zahteva, da se le-ti ohranjajo izključno na ozemlju RS. Takšna zahteva je razumljiva zaradi ozke povezanosti delovanja države ter tako tudi vrste informacijskih sistemov državne informatike z javno varnostjo, kar spada med upravičene izjeme iz − zdaj še predloga − Uredbe o prostem pretoku neosebnih podatkov (predlog Evropske komisije z dne 13. septembra 2017, dostopno na https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/ COM-2017-495-F1-EN-MAIN-PART-1.PDF).

K 18. členu

S predlogom tega člena se ureja priglasitev incidentov za organe državne uprave, in sicer na podoben način, kot 13. člen predloga zakona ureja priglasitve za IBS (glej obrazložitev k predlaganemu 13. členu), s to razliko, da se incidenti s pomembnim vplivom na neprekinjeno izvajanje storitev državnih organov ne priglasijo nacionalnemu CSIRT, kot velja za priglasitve incidentov, prejete od IBS, ampak CSIRT organov državne uprave. Tisti organi državne uprave, ki pa imajo lastne zmogljivosti (vsaj na ravni SOC), pa incidente priglašajo PNO. Glede CSIRT organov državne uprave glej obrazložitev k prehodni določbi 42. člena tega predloga zakona.

6. Standardizacija in prostovoljna priglasitev

Poglavje ureja standardizacijo pristopov zavezancev pri izvajanju njihovih pristojnosti ter vsebuje

določbe glede prostovoljne priglasitve incidentov.

K 19. členu

V predlaganem členu je za uskladitev pristopov IBS, PDS in državnih organov pri izpolnjevanju relevantnih obveznosti v zvezi z zagotavljanjem informacijske varnosti iz predloga zakona v celotni EU PNO podeljena pristojnost spodbujanja uporabe evropskih ali mednarodno sprejetih standardov in specifikacij, pomembnih za varnost omrežij in informacijskih sistemov, pri čemer PNO za ta namen ustrezne informacije objavlja na svoji spletni strani. Gre za prenos prvega odstavka 19. člena Direktive 2016/1148/ES.

K 20. členu

Diskrecija subjektov, ki niso bili določeni za zavezance, in sicer da lahko prostovoljno priglasijo incidente, ki imajo pomemben vpliv na neprekinjeno izvajanje storitev, ki jih zagotavljajo, je opredeljena v predlogu tega člena. Člen napotuje tudi na postopek takšne priglasitve. Gre za prenos 20. člena Direktive 2016/1148/ES. Določeno je tudi, kako mora nacionalni CSIRT ter CSIRT organov državne uprave ravnati s takšnimi priglasitvami v smislu obravnave ter vrstnega reda obravnave.

7. Vrednotenje incidenta, stanje povečane ogroženosti in kibernetska obramba

To poglavje vsebuje določbe o vrednotenju incidenta in ukrepanju, o stanju povečane ogroženosti in ukrepanju ter o obveščanju javnosti, pa tudi določbe o kibernetski obrambi.

K 21. členu

Člen govori o vrednotenju incidentov in ukrepanju v primeru le-teh.

Prvi odstavek ureja pristojnosti za vrednotenje priglašenih incidentov. Za to je pristojen nacionalni CSIRT ali CSIRT organov državne uprave, ki po potrebi sodeluje s PNO. V prvem odstavku so natančneje opredeljeni (kriteriji, razsežnost vpliva, povzročena škoda) lažji, težji in kritični incidenti.

PNO lahko na podlagi podatkov in informacij o teži incidenta oceni, ali gre hkrati tudi za kibernetski napad, kot to določa drugi odstavek.
Tretji odstavek ureja obveznost obveščanja vlade in Sveta za nacionalno varnost (v nadaljnjem besedilu: SNAV) o kritičnem incidentu (lahko pa tudi o težjem incidentu), ki je naložena PNO.
V predlaganem četrtem odstavku je PNO podeljena možnost, da zavezancu zaradi čim hitrejšega in učinkovitega ukrepanja v primeru težjega ali kritičnega incidenta ali v primeru kibernetskega napada s pisno odločbo (v časovni stiski pa tudi ustno) določi takšne ustrezne in sorazmerne ukrepe (ki se skladno s predlaganim petim odstavkom z vidika sorazmernosti določijo v nujno potrebnem obsegu in časovnem terminu), kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic.
V predlaganem šestem odstavku je opredeljena obveznost PNO glede obveščanja vlade in SNAV o ukrepih (določenih v odločbi).

K 22. členu

Člen v prvem odstavku opredeljuje stanje povečane ogroženosti varnosti omrežij ali informacijskih sistemov (v nadaljnjem besedilu: stanje povečane ogroženosti), v drugem odstavku pa PNO podeljuje pristojnost ocenjevanja, ali gre za takšno stanje.
Tretji odstavek določa obveznost PNO glede obveščanja vlade in SNAV o stanju povečane ogroženosti.
V predlaganem četrtem odstavku je, podobno kot v četrtem odstavku 21. člena, podeljena možnost PNO-ju, da lahko IBS ali organu državne uprave z vidika čim hitrejšega in učinkovitega ukrepanja v stanju povišane ogroženosti s pisno odločbo (v časovni stiski pa tudi ustno) določi takšne ustrezne

in sorazmerne ukrepe (ki se skladno s predlaganim petim odstavkom določijo z vidika sorazmernosti v nujno potrebnem obsegu in časovnem terminu), kot je to potrebno za preprečitev ali za zmanjšanje verjetnosti realizacije incidenta.
V predlaganem šestem odstavku je določena obveznost PNO, da vlado in SNAV obvešča o ukrepih (določenih v odločbi).

K 23. členu

Člen vsebuje določbe glede obveščanja javnosti prek medijev. Obveščanje izvaja PNO, skupaj s službo vlade, pristojno za komuniciranje z javnostjo, če je v zvezi s sprejetimi ukrepi iz 21. (vrednotenje incidenta in ukrepanje) ali 22. člena (stanje povečane ogroženosti in ukrepanje) potrebno tudi obveščanje širše javnosti.

K 24. členu

S predlogom člena se postavljajo sistemski okviri za obrambo pred morebitnimi obsežnimi in koordiniranimi kibernetskimi napadi (kibernetski napad je skladno z 12. točko 4. člena tega zakona »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«), ki lahko ogrozijo temeljne državne funkcije ali njene vitalne interese (opredelitve kibernetske obrambe, kibernetske varnosti in kibernetskega napada so navedene v 10., 11. in 12. točkah 4. člena tega predloga zakona). Predlog člena našteva tiste državne organe ali njihove segmente, ki skupaj sodelujejo za namene kibernetske obrambe. Kibernetsko obrambo usklajujejo in izvajajo PNO, nacionalni CSIRT in CSIRT organov državne uprave ter ministrstvo, pristojno za obrambo, policija, Slovenska obveščevalno-varnostna agencija (SOVA) in drugi nacionalni organi skladno s svojimi pristojnostmi pri zagotavljanju nacionalne varnosti, ki za ta namen lahko na različnih ravneh izvajajo usklajene organizacijske, logično-tehnične, tehnične in administrativne ukrepe in dejavnosti za zagotavljanje celovite informacijske varnosti. Pri tem se medsebojno obveščajo in koordinirajo svoje dejavnosti v okviru svojih pristojnosti. V nadaljevanju se kibernetska obramba koordinira tudi v mednarodnem okolju.

8. Seznami

Predlagano poglavje ureja vodenje in vsebino seznamov, ki jih vodijo PNO, nacionalni CSIRT ter CSIRT organov državne uprave.

K 25. členu

Predlog člena v prvih petih odstavkih podeljuje pooblastilo za vodenje seznamov, skupaj z namenom in vsebino le-teh; določene sezname vodijo PNO, nacionalni CSIRT in CSIRT organov državne uprave.
Šesti odstavek opredeli obveznosti PNO, nacionalnega CSIRT in CSIRT organov državne uprave glede priprave anonimiziranih informacij na podlagi seznamov iz tretjega in četrtega odstavka (seznam incidentov in kibernetskih napadov), za statistične namene in seznanjanje javnosti, ki jih tudi javno objavijo na spletnih straneh

9. Organizacija nacionalnega sistema informacijske varnosti

Poglavje vsebuje določbe glede strategije informacijske varnosti, PNO, nacionalnega CSIRT, CSIRT organov državne uprave, SOC ter glede sodelovanja na nacionalni ravni.

K 26. členu

Predlog člena prenaša določbo prvega odstavka 7. člena Direktive 2016/1148/ES o nacionalni strategiji za varnost omrežij in informacijskih sistemov, ki določa, da vsaka država članica sprejme

nacionalno strategijo za varnost omrežij in informacijskih sistemov, v kateri določi strateške cilje ter ustrezne ukrepe politike in regulativne ukrepe, da bi dosegla in vzdrževala visoko raven varnosti omrežja in informacijskih sistemov, pri čemer zajame vsaj področja iz Priloge II (IBS) in storitve iz Priloge III (PDS). Podobno določa tudi Uvodna izjava št. 29.
Glede na navedeno so v predlogu člena določeni obveznost sprejetja strategije informacijske varnosti, njena vsebina, namen, cilj; elementi vsebine, ki jih mora strategija vsebovati, so taksativno našteti.
RS že ima izdelano Strategijo kibernetske varnosti Republike Slovenije, ki jo je vlada sprejela 25. februarja 2016, bo pa po sprejetju zakona to strategijo treba prilagoditi njegovim zahtevam. Tudi sicer je v predlogu zakona v prehodni določbi tretjega odstavka 43. člena predviden časovni okvir za sprejem strategije oziroma prilagoditev strategije določbam tega zakona (najkasneje v roku enega leta od uveljavitve tega zakona).

K 27. členu

Glede na zahteve 8. člena Direktive 2016/1148/ES je v predlaganem členu določen PNO.
V prvem odstavku je določeno, da je PNO organ v sestavi ministrstva, pristojnega za informacijsko družbo (predvidoma bo to tako imenovana »Uprava RS za informacijsko varnost«). Začetek delovanja PNO, pristojnosti Urada Vlade RS za varovanje tajnih podatkov (v nadaljnjem besedilu: UVTP) v vmesnem obdobju ureja prehodna določba 41. člena tega predloga zakona.
V drugem odstavku je določeno, da PNO poleg drugih nalog, določenih v posameznih členih tega predloga zakona, izvaja še druge naloge in jih taksativno našteva. Pri tem na primer koordinira delovanje sistema informacijske varnosti, razvija zmogljivosti za izvajanje kibernetske obrambe, zavezancem nudi strokovno podporo, sodeluje z drugimi pristojnimi organi in organizacijami, je enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in izvaja druge naloge mednarodnega sodelovanja.

K 28. členu

V tem predlogu člena gre za prenos določbe prvega in drugega odstavka 9. člena ter tretjega odstavka 12. člena Direktive 2016/1148/ES.
V prvem odstavku predloga tega člena je določen nacionalni CSIRT, ki je SI-CERT pri Arnes. SI CERT je namreč tudi že trenutno nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Posledično opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah, ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. SI-CERT samostojno izvaja nacionalni program ozaveščanja Varni na internetu in sodeluje v projektu SAFE-SI. Po sklepu vlade št. 38600-3/2009/21 z dne 8. 4. 2010, ter v skladu s sporazumom med Ministrstva za javno upravo (v nadaljnjem besedilu: MJU) z dne 31. 5. 2010, pa SI-CERT opravlja tudi naloge vladnega centra za odzivanje na omrežne incidente. .
V drugem odstavku je določeno, da nacionalni CSIRT poleg drugih nalog, določenih v posameznih členih tega predloga zakona, izvaja še druge naloge in jih taksativno našteva. Prehodna določba (42. člen tega predloga zakona) določa, da nacionalni CSIRT začne z delovanjem po tem zakonu 1. januarja 2019, v tem roku mora tudi izpolniti zahteve iz Priloge I Direktive 2016/1148/ES.

K 29. členu

Pri tem členu gre za nacionalno določbo. V prvem odstavku predloga tega člena določa, da naloge CSIRT organov državne uprave izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave (trenutno je to MJU- glej še prehodno določbo 42. člena, ki navaja rok za vzpostavitev CSIRT organov državne uprave ter da do njegove vzpostavitve njegove naloge opravlja nacionalni CSIRT). Gre za nacionalno določbo.
V drugem odstavku je določeno, da CSIRT organov državne uprave poleg drugih nalog, določenih v posameznih členih tega predloga zakona, izvaja še druge naloge in jih taksativno našteva.

K 30. členu

Člen dopušča IBS, da v sodelovanju in s soglasjem pristojnih organov za področje na katerem delujejo IBS (področja so navedena v drugem odstavku predlaganega 5. člena) vzpostavijo področni SOC, katerega namen je pomoč IBS pri odzivanju na incidente in o ustanovitvi katerega je treba obvestiti PNO (ki jim nudi strokovno pomoč največ dve leti po seznanitvi) ter nacionalni CSIRT. Skladno s tretjim odstavkom lahko organi državne uprave na svojem področju dela vzpostavijo SOC, katerega naloga je, ob sodelovanju s PNO, pomagati tem organom pri odzivanju na incidente.

K 31. členu

Člen prenaša določbe 10. člena Direktive 2016/1148/ES, ki govori o sodelovalni dolžnosti relevantnih organov na nacionalni ravni.

V prvem odstavku se določa sodelovalna dolžnost PNO, in nacionalnega CSIRT ter CSIRT organov državne uprave pri izpolnjevanju obveznosti po tem zakonu.

Drugi odstavek vzpostavlja dolžnost nacionalnega CSIRT in CSIRT organov državne uprave, da PNO (štirikrat letno) poročata o izvajanju svojih nalog, ki jih imata po določbah tega zakona.

Tretji odstavek tem trem organom podeljuje še možnost širšega sodelovanja, in sicer s subjekti v javni upravi, gospodarstvu, z raziskovalno-razvojnimi organizacijami, znanstvenimi institucijami, interesnimi združenji in posamezniki.

10. Nadzor

V tem poglavju predlog zakona ureja področje nadzora, in sicer pristojnosti za nadzor, postopek, pravna sredstva ter upravne ukrepe inšpekcijskega organa. Zaradi različne narave vseh treh kategorij zavezancev (IBS, PDI in organi državne uprave) je, upoštevaje Direktivo 2016/1148/ES (17. člen ter Uvodno izjavo št. 49), za vsakega od njih predvidena specifičen postopek in dovoljen obseg nadzora (glej tudi obrazložitev k 34. členu).

K 32. členu

Predlog člena v prvem odstavku določa pristojnost za nadzor nad izvajanjem določb tega zakona, na njegovi podlagi sprejetih predpisov in upravnih odločb na podlagi tega zakona. Predlagano je, da nadzor opravljajo inšpektorji za informacijsko varnost pristojnega nacionalnega organa (v nadaljnjem besedilu: inšpektor), torej inšpektorji predvidenega novega organa v sestavi ministrstva, pristojnega za informacijsko družbo (predvidoma tako imenovana »Uprava za informacijsko varnost«).

V drugem odstavku je določeno, da lahko inšpektor poleg ukrepov, ki jih ima po zakonu, ki ureja inšpekcijski nadzor (v nadaljnjem besedilu: ZIN) odredi še ukrepe, ki jih ima po tem predlogu zakona.

Tretji odstavek določa sodelovalno dolžnost inšpektorja z Informacijskim pooblaščencem (kar vključuje sodelovanje oziroma obveščanje), kadar v posledici zadev, katere obravnava, je oziroma bi lahko prišlo do kršitve varstva osebnih podatkov ali zgolj suma kršitve. S tem se sledi določbi četrtega odstavka 15. člena Direktive 2016/1148/ES.

V četrtem odstavku je določeno, da se tožba v upravnem sporu zoper dokončno odločbo, izdano v postopku nadzora, vloži pri Upravnem sodišču Republike Slovenije v Ljubljani. V sporu tako odloča Upravno sodišče s sedežem v Ljubljani, kar je z vidika učinkovitosti, upoštevaje specifičnost področja, smotrno. Postopek je zaradi narave zagotavljanja informacijske varnosti in posledic v

odločbi predvidenih ukrepov nujen in prednosten.

K 33. členu

Direktiva 2016/1148/ES vsebuje določbe glede nadzora nad zavezanci tako v Uvodni izjavi kot v členih.

Uvodna izjava št. 49 Direktive 2016/1148/ES določa, da je stopnja tveganja za IBS, ki so pogosto bistvene za ohranjanje ključnih družbenih in gospodarskih dejavnosti, v praksi višja od stopnje tveganja za PDS. Zato bi morale biti varnostne zahteve za PDS manj stroge. PDS bi se tako moralo omogočiti, da se sami odločijo za sprejetje ukrepov, ki se jim zdijo primerni za obvladovanje tveganj, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov. Zaradi čezmejne narave PDS bi se moral zanje uporabljati pristop, usklajen na ravni EU. Z izvedbenimi akti bi morali zagotoviti lažjo določitev in izvajanje tovrstnih ukrepov. Nadalje 17. člen Direktive 2016/1148/ES določa, da pristojni organi naknadne nadzorne ukrepe izvajajo le po potrebi, kadar se jim predložijo dokazi, da PDS ne izpolnjuje zahtev. Inšpektor lahko torej le pod temi pogoji izvaja nadzor nad navedeno kategorijo zavezancev.

Posledično je treba glede pristojnosti za nadzor v skladu s kategorijo zavezanca oblikovati različne režime nadzora.

Predlog tega člena določa pristojnost nadzora nad IBS. Inšpektor lahko nadzira, ali IBS 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 s tem povezane posledice za varnost omrežij in informacijskih sistemov.

Inšpektor lahko od IBS tudi 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 (v zahtevi morata biti navedena namen in opredelitev, katere informacije so potrebne), kar je določeno v drugem odstavku. Na podlagi teh informacij lahko IBS izreka ukrepe za odpravo ugotovljenih pomanjkljivosti.

V tretjem odstavku je navedeno, da se za dokaz o učinkovitem izvajanju varnostnih pravil šteje ocena varnosti omrežij in informacijskih sistemov, ki jo je IBS pripravil skupaj s PNO, ali ocena varnosti, ki jo je za IBS pripravil kvalificiran revizor. Za kvalificiranega revizorja se šteje tisti, ki je certificiran pri ustrezni organizaciji; v RS je to Slovenski inštitut za revizijo.

K 34. členu

Glede na zgoraj (glej obrazložitev k 33. členu) navedeno obveznost delitve oblike oziroma pristojnosti nadzora v skladu s kategorijo zavezanca, upoštevaje Direktivo 2016/1148/ES, je v tem členu določen nadzor nad drugo kategorijo zavezancev − PDS.

Predlog tega člena določa, da inšpektor nadzira, ali PDS izpolnjujejo njihove obveznosti iz prvega, drugega in tretjega odstavka 14. člena tega zakona ter iz odločbe, izdane na podlagi četrtega odstavka 21. člena tega zakona.

V drugem odstavku je predvideno (naknadno) ukrepanje inšpektorja, če so mu predloženi dokazi (dokaze lahko predložijo tudi pristojni organi drugih držav članic EU, v katerih se storitev izvaja), da PDS ne izpolnjuje katerekoli svoje obveznosti. V tem primeru inšpektor izda odločbo, s katero PDS naloži odpravo pomanjkljivosti. Inšpektor ima tako, skladno z že zgoraj (v obrazložitvi k predlaganemu 33. členu) citiranim 17. členom Direktive 2016/1148/ES in Uvodno izjavo št. 49, le pristojnost naknadnega nadzora.

Inšpektor lahko od PDS skladno s četrtim odstavkom tudi zahteva, da predloži informacije in dokaze, potrebne za oceno varnosti njegovega omrežja in informacijskih sistemov, vključno z dokumentiranimi varnostnimi pravili.
V petem odstavku je določeno, da inšpektor v postopkih nadzora po potrebi sodeluje s pristojnimi organi nadzora v drugih državah članicah, če ima PDS svoja omrežja in informacijske sisteme v eni ali več drugih državah članicah EU, kar je zaradi narave opravljanja teh storitev pogosto.
V šestem odstavku je določeno, kako se ravna z izmenjavo informacij in podatkov iz petega odstavka, ki so zaupne narave.

K 35. členu

V tem predlogu člena, ki je nacionalna določba, je določen nadzor nad tretjo kategorijo zavezancev − organi državne uprave.
Inšpektor tako 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 s tem povezane posledice za varnost omrežij in informacijskih sistemov.

Ker glede nadzora nad organi državne uprave veljajo podobne določbe kot glede nadzora nad IBS, se na tem mestu smiselno sklicujemo na obrazložitev k 33. členu.

K 36. členu

Predlog člena določa še dodaten posebni ukrep inšpekcijskega organa, ki ga lahko inšpektor izreka ne glede na ZIN. Inšpektor lahko zavezancem le v skrajnem primeru in upoštevaje področni pomen sistema ter njihovo dejavnost prepove uporabo tega sistema ali njegovega dela, dokler ni ugotovljena pomanjkljivost odpravljena in če s tem ukrepom ni ogrožena zanesljivost oskrbe v posameznem sistemu.

11. Kazenske določbe

V tem poglavju predloga zakona so predpisane kazni za kršitev njegovih določb.

K 37. členu

Glede prekrškovnega postopka se uporabljajo določbe zakona, ki ureja prekrške, vendar je v predlogu člena določena izjema od navedenega zakona, in sicer da se sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem predlogom zakona.

K 38., 39. in 40. členu

V predlogih navedenih členov se določajo globe za vsako kategorijo zavezancev posebej (IBS, PDS ter organi državne uprave), glede na njihovo statusno obliko.
Prekrškovne določbe so tako razdeljene v tri člene, glede na status zavezanca (IBS, PDS ali organ državne uprave). Za IBS (38. člen) in PDS (39. člen) se konkretizira 21. člen Direktive 2016/1148/ES, ki določa, da morajo države članice sprejeti pravila o kaznih za kršitev nacionalnih določb, sprejetih na podlagi te direktive, in vse potrebne ukrepe za zagotovitev, da se te kazni izvajajo; kazni morajo biti učinkovite, sorazmerne in odvračalne. Poleg tega je višina kazni odvisna od statusne oblike in velikosti kršitelja glede na zakon, ki ureja gospodarske družbe. Predvideno je tudi kaznovanje odgovornih oseb kršiteljev.
V zvezi s prekrški državnih organov (40. člen) se z globo kaznuje le odgovorna oseba državnega organa.

12. Prehodne določbe

Predlagano poglavje vsebuje določbe glede začetka delovanja PNO, delovanje drugih pristojnih

organov, izdaje podzakonskih predpisov in strategije ter ukrepanja v prehodnem obdobju.

K 41. členu

Člen ureja začetek delovanja PNO (predvidoma tako imenovana »Uprava RS za informacijsko varnost«), ki začne z delovanjem najkasneje do dne 1. januarja 2020.

S tem dnem 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.
Do pričetka delovanja PNO njegove naloge opravlja UVTP skladno s tem zakonom, razen nalog upravnega odločanja in nadzora, ki jih opravlja ministrstvo, pristojno za informacijsko družbo. Namreč, UVTP kot vladna služba sistemsko ne more izvajati nalog upravnega odločanja in nadzora. Zaradi odložitve pričetka delovanja PNO je potrebno zagotoviti, da se bo ZIV izvajal pred 1. januarjem 2020 v polnem obsegu in skladno z direktivo, ki se prenaša.

K 42. členu

V tem členu se ureja delovanje drugih pristojnih organov, pri čemer nacionalni CSIRT, ki je odzivni center SI-CERT pri Arnes z delovanjem po tem zakonu začne 1. januarja 2019, v tem roku pa mora tudi izpolniti zahteve iz Priloge I Direktive 2016/1148/ES CSIRT organov državne uprave se vzpostavi na ministrstvu, pristojnem za upravljanje informacijsko-komunikacijskih sistemov državne uprave (trenutno je to MJU), najkasneje do 1. januarja 2019, ko ta začne z delovanjem po tem zakonu, do njegove vzpostavitve pa njegove naloge izvaja nacionalni CSIRT.

K 43. členu

Člen določa roke za izdajo obveznih podzakonskih predpisov po tem zakonu in za sprejetje Strategije informacijske varnosti v skladu z določbami tega zakona. Do sprejetja te strategije se uporablja Strategija kibernetske varnosti Republike Slovenije, ki jo je sprejela vlada dne 25. februarja 2016 s sklepom št. 38100-12/2015/5.

K 44. členu

V tem členu so določeni roki za določitev posameznih IBS s strani vlade.
V tem členu je določen tudi rok za izpolnitev obveznosti glede varnostnih zahtev in zahteve za priglasitev skladno s tem zakonom s strani posamezne kategorije zavezancev ter rok za določitev zavezanih organov državne uprave s strani vlade.

13. Končna določba

K 45. členu

V tem členu je določeno, da zakon začne veljati petnajsti dan po objavi v Uradnem listu RS.

IV. BESEDILO ČLENOV, KI SE SPREMINJAJO

/

V. PREDLOG, DA SE PREDLOG ZAKONA OBRAVNAVA PO NUJNEM OZIROMA SKRAJŠANEM POSTOPKU

/

VI. PRILOGE

– Osnutki podzakonskih predpisov.
– Korelacijska tabela.
– Izjava o skladnosti.