OBRAZLOŽITVE K OSNUTKU PREDLOGA

(EVA 2023-1544-0005)

ZAKON

O INFORMACIJSKI VARNOSTI

OBRAZLOŽITEV

PREDSTAVITEV PREDLAGANIH REŠITEV

V nadaljevanju so po poglavjih predstavljene poglavitne rešitve predloga zakona.

I. Splošne določbe

- vsebina predloga zakona ureja področje informacijske in kibernetske varnosti ter opredeljuje nacionalni sistem informacijske varnosti v Republiki Sloveniji, Pri tem ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: pristojni nacionalni organ), organa za obvladovanje incidentov velikih razsežnosti in kriz, enotne kontaktne točke za kibernetsko varnost (v nadaljnjem besedilu: enotna kontaktna točka), skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT), ureja sprejem Strategije kibernetske varnosti Republike Slovenije in določa kibernetsko obrambo ter sodelovanje pristojnih državnih organov in skupin CSIRT);
- predlog zakona zaradi nemotenega delovanja države v vseh varnostnih razmerah ter za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji določa tudi ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznost poročanja zavezancev opredeljenih v predlogu zakona, kar vključuje ter zavezance, ki so določeni kot kritični subjekti v skladu z zakonom, ki ureja področje kritične infrastrukture. Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu;
- namen predloga zakona je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah;
- s tem zakonom se v pravni red Republike Slovenije prenaša Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 333/142, z dne 27. 12. 2022, str.80), (v nadaljnjem besedilu: Direktiva 2022/2555);
- pomen izrazov je skladen z Direktivo 2022/2555, 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 po predlogu zakona se delijo na bistvene in pomembne subjekte;
- zavezanci so javni ali zasebni subjekti vrste iz Prilog zakona Direktive 2022/2555 I ali II (v nadaljnjem besedilu Priloga I ali II), ki ustrezajo prilogama I in II Direktive 2022/2555 in ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov;
- zavezanci so po predlogu zakona ne glede na njihovo velikost ali letni promet oziroma letno bilančno vsoto, kadar:
    - 1. storitev opravljajo:
        - ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev,
        - ponudniki storitev zaupanja,
        - registri vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen;
    - 2. je subjekt edini ponudnik storitve, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti v Republiki Sloveniji;
    - 3. bi motnja pri opravljanju storitve subjekta lahko pomembno vplivala na javni red, javno varnost ali javno zdravje;
    - 4. bi motnja pri opravljanju storitve subjekta lahko povzročila pomembno sistemsko tveganje, zlasti za sektorje, v katerih bi lahko taka motnja imela čezmejni vpliv;
    - 5. je subjekt kritičen zaradi njegovega posebnega pomena na državni, regionalni ali lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v Republiki Sloveniji;
    - 6. gre za subjekt javne uprave na državni ravni ali na regionalni oziroma lokalni ravni, če pri slednjem izhaja iz ocene tveganja, da opravljajo storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti.
- zavezanci po predlogu zakona so tudi subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo; subjekti, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost; povezani subjekti, v kolikor ti niso že zajeti na podlagi prejšnjih odstavkih tega člena ter za subjekte lokalne samouprave in sicer za mestne občine in občine, ki imajo sedeže v krajih, kjer so sedeži upravnih enot;
- pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev. V procesu samoregistracije določijo kontaktno osebo ter sporočijo kontaktne podatke, dodeljene bloke javnih naslovov IP in lastnih domenskih imen za potrebe elektronske pošte; ustrezen sektor in podsektor iz Priloge I ali II v katerem zavezanec izvaja vrste storitev iz teh prilog ali kategorijo zavezancev, ki niso vključeni v navedenih prilogah.

III. Organizacija nacionalnega sistema informacijske varnosti

- strategija kibernetske varnosti (strategija) predstavlja okvir za izvedbo ukrepov za vzpostavitev učinkovitega nacionalnega sistema zagotavljanja informacijske oziroma kibernetske varnosti;
- pristojni nacionalni organ je Urad Vlade Republike Slovenije za informacijsko varnost, ki 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;
- Urad Vlade Republike Slovenije za informacijsko varnost, je tudi pristojni organ za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz;
- za skupini za odzivanje na incidente na področju računalniške varnosti (skupine CSIRTI) sta

določeni CSIRT SI-CERT, ki deluje kot notranja organizacijska enota pri javnem zavodu Akademska in raziskovalna mreža Slovenije in CSIRT državne uprave, ki deluje kot notranja organizacijska enota SIGOV-CERT pri pristojnem nacionalnem organu;
- predlog zakona določa, zahteve in tehnične zmogljivosti skupin CSIRT, njihove naloge ter sodelovanje skupin CSIRT z deležniki zasebnega sektorja;
- CSIRT SI-CERT je koordinator za usklajeno razkrivanje ranljivosti v Republiki Sloveniji (v nadaljnjem besedilu koordinator), ki deluje kot zaupanja vreden posrednik;
- predlog zakona opredeljuje sodelovanje na nacionalni ravni, medsebojni strokovni pregled

IV. Ukrepi za obvladovanje tveganj in priglasitve incidentov

- določeno je upravljanje in odgovornost za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost, ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov
- v skladu z določbami tega zakona odgovorni za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v skladu z določbami tega zakona;
- Zaradi obvladovanja incidentov zagotovijo ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja;
- določena je obveza posredovanja podatkov in informacij, ki jih morajo zavezanci na zahtevo posredovati pristojnemu nacionalnemu organu;
- zaradi zagotavljanja višje ravni kibernetske varnosti zavezanci uporabljajo certifikacijske sheme za kibernetsko varnost in v čim večji meri uporabljajo evropske in mednarodne standarde in tehnične specifikacije;
- zavezanci pristojni skupini CSIRT brez nepotrebnega odlašanja, po predpisanem postopku, priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev;

V. Pristojnost in registracija

- predlog zakona določa pristojnost pristojne skupine CSIRT, za zavezance, ki ji priglašajo incidente, če jih je ustanovila Republika Slovenija ali imajo sedež v Republiki Sloveniji.
- predlog zakona ureja teritorialnost in določa pristojnost v EU ter zbiranje informacij za register ponudnikov storitev pri ENISA ter določa podlago za vzpostavitev podatkovne zbirke o registraciji domenskih imen

VI. Izmenjava informacij

- zavezanci na podlagi tega zakona ter, kadar je to ustrezno, tudi drugi subjekti, si lahko prostovoljno izmenjujejo ustrezne informacije o kibernetski varnosti, vključno z informacijami, ki se nanašajo na kibernetske grožnje, skorajšnje incidente, ranljivosti, tehnike in postopke, kazalnike ogroženosti, sovražne taktike, specifične informacije o grožnji in akterju, opozorila glede kibernetske varnosti in priporočila glede konfiguracije orodij za kibernetsko varnost za zaznavo zlonamernih kibernetskih aktivnosti;
- zavezanci lahko poleg obvezne priglasitve skupinam CSIRT prostovoljno priglasijo incidente, kibernetske grožnje in skorajšnje incidente;
- subjekti, ki niso zavezanci po tem zakonu, ne glede na to, ali spadajo na področje uporabe tega zakona, lahko prostovoljno priglasijo pomembne incidente, kibernetske grožnje in skorajšnje incidente skupini CSIRT SI-CERT.

VII. Vrednotenje incidenta, stanje povečane ogroženosti in kibernetska obramba

- priglašene incidente ob njihovem reševanju vrednoti pristojna skupina CSIRT. V kolikor pristojni

nacionalni organ ugotovi, da ocena ne odraža realnega stanja ali so bila ugotovljena nova dejstva, lahko incident prevrednoti. Varnostne dogodke in incidente se vrednoti v stopnje s poimenovanjem:

- pristojni nacionalni organ na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, s katerimi razpolaga ali jih pridobi, izdela oceno ogroženosti kibernetske varnosti v Republiki Sloveniji;
- pristojni nacionalni organ v primerih, da je ocena ogroženosti ovrednotena kot kritična o tem nemudoma obvesti vlado in SNAV, lahko pa ju, glede na presojo relevantnih okoliščin in informacij, obvesti tudi v primeru, da je ogroženost ovrednotena kot visoka;
- pristojni nacionalni organ zavezancu s pisno odločbo, v nujnih primerih pa tudi ustno, določi primerne in sorazmerne ukrepe, kot je potrebno za zmanjšanje ogroženosti;
- direktor pristojnega nacionalnega organa lahko z namenom nižanja ocene ogroženosti visoka ali kritična ter posledično zaradi preprečitve nastanka krize ali njenega obvladovanja izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih, varnostno operativnih centrih oziroma skupinah CSIRT.

VIII. Kibernetska obramba

- kibernetska obramba vključuje vse plasti kibernetskega prostora, in sicer družbeno, logično-tehnično in fizično;
- ukrepe in dejavnosti kibernetske obrambe na ravni državnih organov usklajujejo in izvajajo pristojni nacionalni organ, skupine CSIRT ter ministrstvo, pristojno za obrambo, ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov, ministrstvo, pristojno za zunanje zadeve, ministrstvo, pristojno za notranje zadeve, policija, Slovenska obveščevalno-varnostna agencija (v nadaljnjem besedilu: SOVA) in drugi nacionalni organi v skladu s svojimi pristojnostmi pri zagotavljanju nacionalne varnost;
- predlog zakona določa sodelovanje na področju kibernetske obrambe vključno s prostovoljnim sodelovanjem državljanov;
- zakon vpeljuje možnost in postopke nudenja pomoči na področju kibernetske obrambe Republiki Sloveniji, znotraj Evropske unije in na mednarodni ravni.
- 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.

IX. 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;
- 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 bistvenimi in pomembnimi subjekti je urejen ločeno (oboje skladno s posebnimi zahtevami iz Direktive 2022/2555).

X. 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 bistveni ali pomembni subjekt ne izpolnjuje obveznosti iz tega zakona, določene v višini, ki je učinkovita, sorazmerna in odvračalna (skladno z zahtevo iz Direktive 2022/2555);
- predlog zakona ločeno ureja prekrške v primerih, ko obveznosti tega zakona ne izpolnjujejo bistveni ali pomembni subjekti. Ločeno je tudi urejanje prekrškov upravljavca centralnega informacijsko-komunikacijskega sistema.

XI. Prehodne določbe

- določa določbe, ki urejajo, kako se bodo zakon in predpisi uporabljal v prehodnem obdobju po njegovi uveljavitvi ali spremembi.

XII. Končna določba

- določa začetek veljavnosti zakona − petnajsti dan po objavi v Uradnem listu RS.

OBRAZLOŽITVE K OSNUTKU PREDLOGA

PREDSTAVITEV ČLENOV

I. Splošne določbe

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

K 1. členu

Predlog člena opredeljuje vsebino zakona, ki predstavlja sistemsko osnovo za celovito ureditev informacijske in kibernetske varnosti na določenih ključnih področjih v Republiki Sloveniji.
Predlog zakona tako ureja področje informacijske in kibernetske varnosti ter opredeljuje nacionalni sistem informacijske varnosti v Republiki Sloveniji. Pri tem ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost (v nadaljnjem besedilu: pristojni nacionalni organ), organa za obvladovanje incidentov velikih razsežnosti in kriz, enotne kontaktne točke za kibernetsko varnost (v nadaljnjem besedilu: enotna kontaktna točka), skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT); ureja sprejem Strategije kibernetske varnosti Republike Slovenije in določa kibernetsko obrambo ter sodelovanje pristojnih državnih organov in skupin CSIRT.
Zakon zaradi nemotenega delovanje države v vseh varnostnih razmerah ter za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji določa tudi ukrepe za obvladovanje tveganj za kibernetsko varnost in obveznost poročanja zavezancev po tem zakonu. . Ureja tudi pravila in obveznosti glede izmenjave informacij o kibernetski varnosti ter nadzor po tem zakonu.
Predlagana določba pri tem vključuje tudi vsebine iz 1. člena (Predmet urejanja) Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 333/142, z dne 27. 12. 2022, str.80), nazadnje popravljena s Popravkom Direktive (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) š. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (Direktiva NIS 2) (UL L št. 239 z dne 28. 9. 2023, str. 48) (v nadaljnjem besedilu: Direktiva 2022/2555).

K 2. členu

Predlog člena v prvem odstavku pojasnjuje namen predloga zakona, ki je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji na področjih, ki so bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah.
Drugi odstavek člena določa, da se s tem zakonom v pravni red Republike Slovenije prenaša Direktiva 2022/2555..
Ob tem je treba pojasniti, da predlagani zakon ob upoštevanju njegovega namena iz prvega odstavka predlaganega člena poleg prenosa Direktive 2022/2555 sistemsko ureja področje informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti v Republiki Sloveniji tudi na področjih, ki niso zajeta z Direktivo 2022/2555 (ki je direktiva notranjega trga ter direktiva minimalne harmonizacije), so pa bistvenega pomena za nemoteno delovanje države ter ohranitev zagotavljanja ključnih družbenih in gospodarskih dejavnosti v vseh varnostnih razmerah. V tem smislu predlagani zakon sledi sistemskemu načinu urejanja iz Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV), ki ga nadomešča. Predlagani zakon vsebuje torej tudi nacionalne določbe, ki so potrebne za zagotovitev namena predstavljenega v prvem odstavku tega člena.

OBRAZLOŽITVE K OSNUTKU PREDLOGA

K 3. členu

S predlogom tega člena se določa področje uporabe predlaganega zakona. Pri tem predlagani člen v pretežni meri sledi 2. členu (Področje uporabe) Direktive 2022/2555, vendar ob upoštevanju nacionalnih pristojnosti urejanja na področjih, ki niso bila pogodbeno prenesena na Evropsko Unijo (v nadaljnjem besedilu: Unija) in jih predmetna direktiva (ki je direktiva notranjega trga) zato izključuje iz področja svoje uporabe. Posledično predlagani zakon ne izključuje v celoti njegove uporabe za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, kot to izhaja iz sedmega odstavka Direktive 2022/2555, upošteva pa se šesti odstavek Direktive 2022/2555, po katerem ta direktiva ne posega v pristojnosti držav članic, da zaščitijo nacionalno varnost, in v njihova pooblastila za zaščito drugih bistvenih državnih funkcij, vključno z zagotavljanjem ozemeljske celovitosti države ter vzdrževanjem javnega reda in miru. Pri tem uvodna izjava 13 prej navedene direktive pojasnjuje: »Glede na okrepitev in večjo izpopolnjenost kibernetskih groženj bi si morale države članice prizadevati zagotoviti, da subjekti, ki so izključeni s področja uporabe te direktive, dosežejo visoko raven kibernetske varnosti, in podpirati izvajanje enakovrednih ukrepov za obvladovanje tveganj za kibernetsko varnost, ki odražajo občutljivo naravo teh subjektov.«. Upoštevajo se tudi določbe 5. člena Direktive 2022/2555 (Minimalna harmonizacija), po kateri ta direktiva državam članicam ne preprečuje, da sprejmejo ali ohranijo določbe, ki zagotavljajo višjo raven kibernetske varnosti, pod pogojem, da so take določbe v skladu z obveznostmi držav članic, določenimi v pravu Unije.
Ob tem pa že Direktiva 2022/2555 v uvodni izjavi šest pojasni, da bi bilo z razveljavitvijo Direktive (EU) 2016/1148[1], treba področje uporabe po sektorjih razširiti na večji del gospodarstva, da bi se zagotovila celovita pokritost sektorjev in storitev, ki so bistvenega pomena za ključne družbene in gospodarske dejavnosti na notranjem trgu. Ta širitev področja uporabe po sektorjih je razvidna iz Priloge I (Visoko kritični sektorji) in Priloge II (Drugi kritični sektorji) Direktive 2022/2555, ki naštevata sektorje, v določenih primerih pa tudi podsektorje, znotraj katerih delujejo v obeh prilogah naštete vrste subjektov, kar je relevantno z vidika področja uporabe te direktive. Pri tem Direktiva 2022/2555, kot osnovno pravilo (od katerega v nekaterih primerih odstopa) postavlja pravilo velikosti. Glede prej navedenega uvodna izjava sedem Direktive 2022/2555 pojasnjuje: »Na podlagi Direktive (EU) 2016/1148 so bile države članice odgovorne za določitev subjektov, ki izpolnjujejo merila, na podlagi katerih se štejejo za izvajalce bistvenih storitev. Za odpravo velikih razlik med državami članicami v zvezi s tem in zagotovitev pravne varnosti v zvezi z ukrepi kibernetske varnosti za obvladovanje tveganja in obveznosti poročanja za vse ustrezne subjekte bi bilo treba določiti enotno merilo, ki bi določalo, kateri subjekti spadajo na področje uporabe te direktive. To merilo bi moralo vključevati uporabo pravila omejitve velikosti, v skladu s katerim na področje uporabe te direktive spadajo vsi subjekti, ki se na podlagi člena 2 Priloge k Priporočilu Komisije 2003/361/ES[2] štejejo za srednja podjetja, ali presegajo zgornje meje za srednja podjetja iz odstavka 1 navedenega člena, in ki delujejo v sektorjih in opravljajo vrste storitev ali izvajajo dejavnosti, zajete s to direktivo. Države članice bi morale tudi zagotoviti, da na področje uporabe te direktive spadajo nekatera mala podjetja in mikropodjetja, kot so opredeljena v členu 2(2) in (3) navedene priloge, ki izpolnjujejo posebna merila, ki kažejo na ključno vlogo za družbo, gospodarstvo ali za določene sektorje ali vrste storitev.«.
Določba prvega odstavka 2. člena Direktive 2022/2555 kot splošno pravilo njenega področja uporabe zato določa, da se ta direktiva uporablja za javne ali zasebne subjekte vrste iz Priloge I ali II navedene direktive, ki izpolnjujejo pogoje za srednja podjetja iz člena 2 Priloge Priporočilu 2003/361/ES, ali presegajo zgornje meje za srednja podjetja, določene v odstavku 1 navedenega člena, in ki opravljajo svoje storitve ali izvajajo svoje dejavnosti v Uniji. Člen 3(4) Priloge k navedenemu priporočilu pa se ne uporablja za namene te direktive. Navedeno splošno pravilo področja uporabe se prenaša v predlagani zakon s prvim odstavkom predlaganega člena, po katerem se ta zakon uporablja za javne ali zasebne

[1] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).
[2] Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

subjekte vrste iz Prilog predlaganega zakona I ali II (v nadaljnjem besedilu Priloga I ali II), ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov, kar ustreza kriterijem te direktive in priporočila, na katerega se sklicuje.Drugi odstavek predlaganega člena določa primere, kot se predlagani zakon uporablja za subjekte iz prejšnjega odstavka (gre torej za subjekte vrste iz Priloge I ali II) ne glede na njihovo velikost ali letni promet oziroma letno bilančno vsoto in sicer, kadar: 1. opravljajo storitev ponudnika javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ponudniki storitev zaupanja ali registra vrhnjih domenskih imen in ponudniki storitev sistema domenskih imen; 2. je subjekt edini ponudnik storitve, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti v Republiki Sloveniji; 3. bi motnja pri opravljanju storitve subjekta lahko pomembno vplivala na javni red, javno varnost ali javno zdravje; 4. bi motnja pri opravljanju storitve subjekta lahko povzročila pomembno sistemsko tveganje, zlasti za sektorje, v katerih bi lahko taka motnja imela čezmejni vpliv; 5. je subjekt kritičen zaradi njegovega posebnega pomena na državni, regionalni ali lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v Republiki Sloveniji; 6. gre za subjekt javne uprave na državni ravni ali na regionalni oziroma lokalni ravni, če pri slednjem izhaja iz ocene tveganja, da opravljajo storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti. Ta predlagana določba pomeni prenos drugega odstavka 2. člena Direktive 2022/2555. Z vidika možnosti nacionalne širitve se pri točkah 5 in 6 dodaja še lokalna raven, namreč po točki (a) petega odstavka 2. člena Direktive 2022/2555, države članice lahko določijo, da se ta direktiva uporablja tudi za subjekte javne uprave na lokalni ravni. Republika Slovenija trenutno (še) nima regionalne ravni lokalne samouprave, se jo pa vključuje v predlagani zakon skladno z Direktivo 2022/2555. V primeru vzpostavitve regionalne samouprave tako ne bo treba zgolj iz tega razloga dopolnjevati sedaj predlagane zakonske ureditve. Prav tako se z vidika možnosti nacionalne širitve na tem mestu dodaja še točka 7 in sicer, kadar gre za subjekt javne uprave na lokalni ravni, če pri slednjem izhaja iz njegove ocene tveganja, da opravlja storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti.

Tretji odstavek predlaganega člena določa, da se ta zakon uporablja tudi za subjekte, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo, torej gre za vse subjekte, ki so tako določeni, ne glede na njihovo velikost. Pri tem gre za prenos tretjega odstavka 2. člena Direktive 2022/2555, ki določa, da se ta direktiva uporablja tudi za subjekte, ki so identificirani kot kritični na podlagi Direktive (EU) 2022/2557[3], ne glede na njihovo velikost, pri čemer se ta direktiva istočasno prenaša v slovenski pravni red z (novim) zakonom, ki ureja kritično infrastrukturo.

Četrti odstavek predlaganega člena določa, da se ta zakon uporablja tudi za subjekte, ki opravljajo storitve registracije domenskih imen, ne glede na njihovo velikost, kar je prenos četrtega odstavka 2. člena 2022/2555.

Peti odstavek predlaganega člena je nacionalna določba, ki upoštevaje 5. člen Direktive 2022/2555 (minimalna harmonizacija) širi področje uporabe zakona še na tako imenovane povezane subjekte (ki se jih opredeljuje med zakonskimi izraz), v kolikor takšni subjekti niso že zajeti med subjekti, za katere se uporablja ta zakon, na podlagi prejšnjih odstavkov tega člena. Pri tem se upošteva, da je t.i. povezane subjekte med zavezance vključila že zadnja novela ZInfV, kar se ohranja tudi v sklopu predlaganega zakona, z namenom ohranitve že dosežene ravni informacijske in kibernetske varnosti v Republiki Sloveniji.

Šesti odstavek predlaganega člena določa uporabo tega zakona tudi za subjekte lokalne samouprave in sicer za mestne občine in občine, ki imajo sedeže v krajih, kjer so sedeži upravnih enot, pri čemer se upošteva točka (a) petega odstavka 2. člena Direktive 2022/2555, po kateri države članice lahko določijo, da se ta direktiva uporablja tudi za subjekte javne uprave na lokalni ravni.

Sedmi odstavek tega člena določa, da se zakon ne uporablja za subjekte, ki jih je Republika Slovenija izvzela s področja uporabe Uredbe (EU) 2022/2554 v skladu s četrtim odstavkom 2. člena prej navedene uredbe. Navedeno ustreza desetemu odstavku 2. člena Direktive 2022/2555, po katerem se ta direktiva

[3] Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljaviti Direktive Sveta 2008/114/ES (UL L št. 333/142, z dne 27. 12. 2022, str. 164).

ne uporablja za subjekte, ki so jih države članice izvzele s področja uporabe Uredbe (EU) 2022/2554[4] v skladu s členom 2(4) navedene uredbe.
Po osmem odstavku predlaganega člena ta zakon ne posega v izvajanje predpisov s področja varstva osebnih podatkov in zasebnosti na področju elektronskih komunikacij, s področja boja proti spolni zlorabi otrok in proti izdelavi, razširjanju in hrambi gradiva, ki prikazuje spolno zlorabo otrok, predpisa o napadih na informacijske sisteme in s področja kritične infrastrukture. Navedeno ustreza dvanajstemu odstavka 2. člena Direktive 2022/2555, po katerem se ta direktiva med drugim uporablja brez poseganja v direktivi 2011/93/EU[5] in 2013/40/EU[6].
Pri devetem, desetem in enajstem odstavku predlaganega člena gre za prenos člena 4 (Sektorski pravni akti Unije) Direktive 2022/2555, ki v prvem odstavku določa pravila in pogoje za izključitev iz uporabe zadevnih določb te direktive za bistvene ali pomemben subjekte, ki bi sicer spadali v njeno področje uporabe, pa sektorski pravni akti Unije za njih vsebujejo po učinku vsaj enakovredne zahteve bodisi za obvladovanje tveganj za kibernetsko varnost bodisi za priglasitev incidentov. Pri tem je v drugem odstavku 4. člena določeno tudi, kdaj se takšne zahteve štejejo za enakovredne zahtevam te direktive, v tretjem odstavku pa so bile napovedane tudi Smernice Evropske komisije o uporabi prvega in drugega odstavka tega člena, ki so bile medem že sprejete[7]. Že uvodni izjavi 28 in 29 Direktive 2022/2555 pa glede takšne po učinku enakovredne sektorske zakonodaje podajata primera, ki se nanašata na finančni sektor ter na letalski sektor in se glasita:
»(28) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta (10) bi se morala šteti za sektorski pravni akt Unije v zvezi s to direktivo, kar zadeva finančne subjekte. Določbe Uredbe (EU) 2022/2554 v zvezi z ukrepi za obvladovanje tveganj na področju informacijske in komunikacijske tehnologije (IKT), obvladovanjem incidentov, povezanih z IKT, in zlasti poročanjem o večjih incidentih, povezanih z IKT, kot tudi testiranjem digitalne operativne odpornosti, dogovori o izmenjavi informacij in tveganjem tretjih oseb na področju IKT bi se morale uporabljati namesto določb te direktive. Države članice zato ne bi smele uporabljati določb te direktive o obvladovanju tveganj za kibernetsko varnost in obveznostih poročanja ter nadzoru in izvrševanju za finančne subjekte, zajete z Uredbo (EU) 2022/2554. Hkrati je pomembno ohranjati tesno povezavo in izmenjavo informacij s finančnim sektorjem na podlagi te direktive. V ta namen Uredba (EU) 2022/2554 evropskim nadzornim organom in pristojnim organom iz navedene uredbe omogoča, da sodelujejo pri dejavnostih skupine za sodelovanje ter si izmenjujejo informacije in sodelujejo z enotnimi kontaktnimi točkami, kot tudi s skupinami CSIRT in pristojnimi organi iz te direktive. Pristojni organi iz Uredbe (EU) 2022/2554 bi morali podrobnosti o večjih incidentih, povezanih z IKT, in po potrebi pomembnih kibernetskih grožnjah posredovati tudi skupinam CSIRT, pristojnim organom ali enotnim kontaktnim točkam iz te direktive. To je mogoče doseči z zagotovitvijo takojšnjega dostopa do priglasitev incidentov in njihovega posredovanja neposredno ali prek enotne vstopne točke. Poleg tega bi morale države članice še naprej vključevati finančni sektor v svoje strategije za kibernetsko varnost, skupine CSIRT pa lahko vključijo finančni sektor v svoje dejavnosti.
(29) V izogib vrzelim ali podvajanju obveznosti glede kibernetske varnosti, ki veljajo za subjekte v letalskem sektorju, bi morali nacionalni organi iz uredb (ES) št. 300/2008 (11) in (EU) 2018/1139 (12) Evropskega parlamenta in Sveta ter pristojni organi iz te direktive sodelovati pri izvajanju ukrepov za obvladovanje tveganj za kibernetsko varnost in nadzoru spoštovanja teh ukrepov na nacionalni ravni. Pristojni organi iz te direktive bi lahko skladnost subjekta z varnostnimi zahtevami iz uredb (ES) št. 300/2008 in (EU) 2018/1139 ter iz ustreznih delegiranih in izvedbenih aktov, sprejetih na podlagi navedenih uredb, šteli za skladnost z ustreznimi zahtevami iz te direktive.«

[4] Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti v finančnem sektorju in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L št. 333/142, z dne 27. 12. 2022, str. 1).
[5] Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL L 335, 17.12.2011, str. 1).
[6] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).
[7] Gre za Sporočilo Komisije - Smernice Komisije o uporabi člena 4 (1) in (2) Direktive (EU) 2022/2555 (Direktiva NIS) (UL C 328, z dne 18. 9. 2023, str. 2)

OBRAZLOŽITVE K OSNUTKU PREDLOGA

K 4. členu

Določba štirinajstega odstavka 2. člena Direktive 2022/2555, določa, da subjekti, pristojni organi, enotne kontaktne točke in skupine CSIRT obdelujejo osebne podatke v obsegu, ki je potreben za namene te direktive, in v skladu z Uredbo (EU) 2016/679 (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov)[8], pri čemer mora taka obdelava zlasti temeljiti na členu 6 Uredbe. Kar zadeva obdelavo osebnih podatkov na podlagi te direktive, jo morajo ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev izvajati v skladu s pravom Unije o varstvu podatkov in pravom Unije o zasebnosti, zlasti z Direktivo 2002/58/ES (v nadaljnjem besedilu: Direktiva o zasebnosti in elektronskih komunikacijah)[9]. Uvodna izjava 14 Direktive 2022/2555 se pri tem glasi: »Pravo Unije o varstvu podatkov in pravo Unije o zasebnosti se uporablja za vsakršno obdelavo osebnih podatkov na podlagi te direktive. Ta direktiva zlasti ne posega v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ter Direktivo 2002/58/ES Evropskega parlamenta in Sveta. Ta direktiva zato med drugim ne bi smela vplivati na naloge in pooblastila organov, pristojnih za spremljanje skladnosti z veljavnim pravom Unije o varstvu podatkov in pravom Unije o zasebnosti.«.
Zato prvi odstavek predlaganega člena najprej določa, da se obdelava osebnih podatkov na podlagi tega zakona izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev pa jo izvajajo tudi v skladu s predpisom, ki ureja zasebnosti na področju elektronskih komunikacij. Pri tem pojasnjujmo, da Direktivo o zasebnosti in elektronskih komunikacijah v slovenski pravni red prenaša zakon, ki ureja elektronske komunikacije, trenutno je to Zakon o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2) v svojem XII. poglavju, ki ima naslov »OBEDELAVA OSEBNIH PODATKOV IN VARSTNO ZASEBNOSTI ELEKTRONSKIH KOMUNIKACIJ«. Pri tem že prvi člen tega poglavja (to je 211. člen ZEKom-2) v tretjem odstavku pojasni, da to poglavje ureja obdelavo osebnih podatkov v zvezi z zagotavljanjem javnih komunikacijskih storitev v javnih komunikacijskih omrežjih, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave. Med predpise s področja varstva osebnih podatkov poleg Splošne uredbe o varstvu podatkov v slovenskem pravnem redu spada predvsem Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22: v nadaljnjem besedilu: ZVOP-2). Nadalje se v predlagani določbi prvega odstavka tega člena zaradi jasnosti še določa, da obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij pomeni zakoniti interes zadevnega upravljavca podatkov. Pri tem smo izhajali iz uvodne izjave 49 Splošne uredbe o varstvu podatkov, ki pojasnjuje: »Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežja in informacij, tj. zmožnosti omrežja ali informacijskega sistema, da na določeni ravni zaupanja prepreči slučajne dogodke ali nezakonita ali zlonamerna dejanja, ki ogrožajo dostopnost, avtentičnost, celovitost in zaupnost shranjenih ali prenesenih osebnih podatkov ter varnost s tem povezanih storitev, ki jih ponujajo ali so dostopne prek teh omrežij in sistemov, s strani javnih organov, skupin za odzivanje na računalniške grožnje, skupin za odzivanje na računalniške varnostne incidente, ponudnikov elektronskih komunikacijskih omrežij in storitev ter ponudnikov varnostnih tehnologij in storitev pomeni zakoniti interes zadevnega upravljavca podatkov. To bi lahko vključevalo na primer preprečevanje nepooblaščenega dostopa do elektronskih komunikacijskih omrežij, širjenja zlonamernih kod, napadov, ki povzročajo zavrnitev storitve, ter škode na računalniških in elektronskih komunikacijskih sistemih.«.
V nadaljevanju predlagani člen ob upoštevanju nacionalnih posebnosti v predlagani zakon prenaša trinajsti odstavek 2. člena Direktive 2022/2555, ki določa: »Brez poseganja v člen 346 PDEU se informacije, ki so zaupne v skladu s predpisi Unije ali nacionalnimi predpisi, na primer o poslovni tajnosti, s Komisijo in drugimi ustreznimi organi v skladu s to direktivo izmenjajo le, kadar je takšna izmenjava

[8] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).
[9] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

potrebna za uporabo te direktive. Izmenjava informacij se omeji na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave. Pri izmenjavi informacij se ohrani zaupnost zadevnih informacij ter zaščitijo varnost in poslovni interesi zadevnih subjektov.«. Posledično je v drugem odstavku predlaganega člena z vidika varstva zaupnosti podatkov in informacij, ki se obdelujejo na podlagi predlaganega zakona in so opredeljeni kot tajni ali kot poslovna skrivnost ali druge oblike varovanih podatkov, predlagano, da se le-ti obravnavajo v skladu s področnimi predpisi, ki urejajo njihovo obravnavo in varovanje. Pri tem gre zlasti za zakon, ki ureja varstvo tajnih podatkov, pa tudi za druge področne zakone, ki urejajo obravnavo in varovanje npr. davčne ali bančne tajnosti, posebnosti predpisov na področju zunanjih zadev, urejanje poslovne skrivnosti v skladu z zakonom, ki ureja gospodarske družbe in podobno. Izmenjava podatkov in informacij, ki so opredeljeni kot tajni ali poslovna skrivnost mora biti za potrebe izvajanja tega zakona v vsakem primeru omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij ter zaščiti varnost in poslovni interes zadevnih subjektov.
Novost (glede na ZInfV) je določba tretjega odstavka predlaganega člena, ki določa pravila za izmenjavo podatkov in informacij, ki so varovani podatek pristojnega nacionalnega organa. Izmenjava podatkov in informacij, ki so varovani podatek pristojnega nacionalnega organa, mora biti za potrebe izvajanja tega zakona namreč omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij ter zaščiti varnost in poslovni interes zadevnih subjektov. Ne glede na določbe zakona, ki ureja dostop do informacij javnega značaja, se predlaga, da se varovani podatki pristojnega nacionalnega organa ne posredujejo javnosti.
Nadalje se s predlaganim četrtem odstavkom tega člena določa, da se pri posredovanju ali izmenjavi podatkov in informacij na podlagi tega zakona upošteva tudi sporazume o nerazkritju informacij in neformalne sporazume o nerazkritju informacij, kot je semaforski protokol, kar je novost glede na ZInfV, ki se v praksi, kot to navaja tudi uvodna izjava 9 Direktive 2022/2555/EU na koncu besedila, že uporablja v skoraj vseh skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter v nekaterih centrih za analizo in izmenjavo informacij. Kot to pojasnjuje navedena uvodna izjava je pri tem semaforski protokol (Traffic Light Protocol) treba razumeti kot sredstvo za zagotavljanje informacij o kakršnih koli omejitvah v zvezi z nadaljnjim širjenjem informacij.
Ne glede na vse zgoraj opisane omejitve pri posredovanju ali izmenjavi zaupnih informacij pa peti odstavek prinaša še izrecno varovalko, po kateri obveznost izmenjave podatkov na podlagi tega zakona ne vključujejo posredovanja podatkov in informacij, katerih razkritje bi bilo v nasprotju z vitalnimi interesi Republike Slovenije na področju nacionalne varnosti, javne varnosti ali obrambe, izven Republike Slovenije. Tudi prej navedena uvodna izjava 9 navaja, da se od nobene države članice ne bi smelo zahtevati, da daje informacije, katerih razkritje bi bilo v nasprotju z bistvenimi (v našem pravnem redu se uporablja termin »vitalnimivitalnim«i) interesi njene nacionalne varnosti, javne varnosti ali obrambe. Ocenjujemo, da je takšna izrecna varovalka potrebna, saj predlagani zakon ne izključuje njegove uporabe za subjekte javne uprave, ki izvajajo svoje dejavnosti na področju nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj, kot je to pojasnjeno zgoraj v obrazložitvah k 1. ter zlasti k 2. členu predlaganega zakona. Vendar pa je ob ne izključitvi področja uporabe za zadevne subjekte hkrati treba upoštevati njihovo občutljivo naravo.

K 5. členu

V predlogu člena se pojasnjujejo uporabljeni izrazi; opredelitve izrazov so večinoma povzete po Direktivi 2022/2555 (njen 6. člen), v delu, ko gre za nacionalne določbe, pa po opredelitvah strokovnih pojmov s področja informacijske in kibernetske varnosti oziroma obramboslovja.

II. Zavezanci

V tem poglavju so navedeni zavezanci (za izpolnjevanje obveznosti) po predlaganem zakonu, ureja se mehanizem za njihovo samoregistracijo in podlaga za vodenje seznama zavezancev po tem zakonu.

K 6. členu

V predlogu člena se določajo zavezanci za izpolnjevanje obveznosti po predlaganem zakonu, Predlagani člen pri tem ob upoštevanju člena 5 Direktive 2022/2055 (minimalna harmonizacija) v predlagani zakon prenaša člen 3 Direktive 2022/255 (bistveni in pomembni subjekti). Pri tem prvi odstavek predlaganega člena uvodno pojasnjuje, da se zavezanci delijo na bistvene in pomembne subjekte.
Predlog člena v drugem odstavku določa, da se za namene tega zakona šteje, da so bistveni subjekti: (1) subjekti vrste iz Priloge I, ki imajo vsaj 250 zaposlenih in letni promet vsaj 50 milijonov evrov oziroma letno bilančno vsoto vsaj 42 milijonov evrov; (2) ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost; (3) ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov; (4) subjekti javne uprave na državni ravni; (5) vsi drugi subjekti vrste iz Prilog I ali II, ki jih , na podlagi 2. do 5. točke drugega odstavka 3. člena tega zakona, in na predlog pristojnega nacionalnega organa določi vlada z odločbo; (6) subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo (7) subjekti, ki so bili v skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023; in (8) drugi subjekti, ki niso subjekti iz točk 1 do 7 tega odstavka, ki jih vlada lahko določi kot bistvene subjekte zaradi pomembnega negativnega vpliva, ki bi ga incident pri izvajanju njihovih storitev imel za življenje in zdravje ljudi oziroma zaradi pomembnega negativnega vpliva na okolje. Pri prvih sedmih točkah gre za prenos določb oziroma možnosti iz prvega odstavka 3. člena Direktive 2022/2555 in sicer točk od (a) do (g) v predlagani zakon. Zadnja, to je 8. točka, je nacionalne narave in predstavlja dodatno možnost za določitev posameznega subjekta (ki spada v področje uporabe tega zakona po 3. členu predlaganega zakona) za bistveni subjekt.
Tretji odstavek predlaganega člena v skladu drugim odstavkom 3. člena Direktive 2022/2555 določa pomembne subjekte, ki so subjekti vrste iz Prilog I ali II in drugi subjekti iz 3. člena predlaganega zakona, ki se ne štejejo za bistvene subjekte na podlagi prejšnjega odstavka. Gre torej za vse ostale subjekte, ki spadajo v področje uporabe predlaganega zakona in niso opredeljeni bistveni subjekti.
Četrti odstavek predlaganega člena pooblašča vlado, da izvajanje 8. točke drugega odstavka tega člena lahko podrobneje opredeli z metodologijo za določitev zadevnih subjektov kot bistvenih.

K 7. členu

Predlog člena prenaša določbe tretjega, četrtega in petega odstavka 3. člena Direktive 2022/2555. Te določbe direktive v tretjem odstavku določajo dolžnost držav članic, da oblikujejo seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen in ga redno (vsaj vsaki dve leti) pregledajo in po potrebi posodijo. Države članice za namene priprave takšnega seznama od teh subjektov zahtevajo vsaj informacije naštete v četrtem odstavku prej navedene določbe, ki jih morajo subjekti tudi posodabljati po nastali spremembi, pri čemer države članice lahko vzpostavijo nacionalne mehanizme za samoregulacijo subjektov. Peti odstavek prej navedene določbe direktive pa pristojnim (nacionalnim) organom nalaga dolžnost in roke za obveščanje Evropske komisije o številu bistvenih in pomembnih subjektov, ki so na seznamu v posledici različnih določb navedene direktive. Šesti odstavek navedenega člena direktive pa daje možnost državam članicam, da lahko Evropsko komisijo na njeno zahtevo obveščajo tudi o imenih nekaterih takšnih subjektov, pri čemer takšna možnost v predlogu tega zakona ni bila uporabljena.

OBRAZLOŽITVE K OSNUTKU PREDLOGA

Predlog tega čelna prej navedene določbe Direktive 2022/2555 prenaša na način, da v prvem odstavku predlaganega člena najprej nalaga pristojnemu nacionalnemu organu, da vzpostavi mehanizem za samoregistracijo zavezancev iz prejšnjega (to je 6.) člena.

Drugi odstavek predlaganega člena nato nalaga zavezancem iz prejšnjega (to je 6.) člena predlaganega zakona, da se morajo registrirati preko mehanizma za samoregistracijo ter določa, katere informacije morajo ob tem podati. Pri tem se ob upoštevanju načela minimalne harmonizacije iz 5. člena Direktive 2022/2555 v interesu učinkovitejšega sodelovanja med pristojnim nacionalnim organom in zavezanci ter višanja ravni zagotavljanja informacijske in kibernetske varnosti nekoliko širi nabor informacij, ki jih kot minimalne določa Direktiva 2022/2555.

Tretji odstavek določa obveznost, da zavezanci nemudoma oziroma vsaj v dveh tednih sporočijo morebitne spremembe podatkov, ki so jih podali ob samoregistraciji.

Podlaga za vodenje seznama subjektov iz prvega odstavka predlaganega člena izhaja iz četrtega odstavka, ki določa, da pristojni nacionalni organ vzpostavi seznam bistvenih in pomembnih subjektov ter subjektov, ki opravljajo storitve registracije domenskih imen. Do seznama imajo po predlogu petega dostavka dostop pristojne skupine CSIRT. Pristojni nacionalni organ Evropsko komisijo, v določenih primerih pa tudi Skupino za sodelovanje, obvešča o številu bistvenih in pomembnih subjektov.

Zaradi lažjega izvajanja oziroma upoštevanja določb 4. člena (Sektorski pravni akti Unije) Direktive 2022/2555, ki so sicer prenesene z devetim, desetim in enajstim odstavkom 3. člena predlaganega zakona, se na tem mestu predlaga, da organi, ki so pristojni za izvajanje področnih predpisov iz devetega odstavka 3. člena tega zakona, v 30 dneh od uveljavitve takšnega področnega predpisa seznanijo pristojni nacionalni organ z identiteto subjektov (ime in naslov) s področja njihove pristojnosti, ki so na podlagi prej navedene določbe izključeni s področja uporabe zadevnih določb tega zakona ter o izpolnjevanju pogojev za takšno izključitev iz desetega odstavka 3. člena tega zakona. Namreč področne predpise, kar vključuje tako neposredno uporabljive predpise EU, kot tudi morebitne nacionalne predpise, ki prenašajo EU zakonodajo ali pa so potrebni z vidika njenega izvajanja v Republiki Sloveniji ter tudi zavezance za izpolnjevanje obveznosti po teh področnih predpisih najbolje poznajo organi, ki so pristojni za izvajanje takšnih področnih predpisov. Zato je najbolj primerno, da oni ustrezno obvestijo pristojni nacionalni organ, da ne bi v takšnih primerih prišlo do nepotrebnih nadzornih postopkov in sankcioniranja po predlaganem zakonu (morebiti že iz razloga, ker ni prišlo do samoregistracije takšnega subjekta). Pristojni nacionalni organ pa z organi pristojnimi za izvajanje takšnih področnih predpisov sodeluje na podlagi 5. točke 9. člena in 17. člena tega zakona.

III. Organizacija nacionalnega sistema informacijske varnosti

Poglavje vsebuje določbe glede strategije kibernetske varnosti, pristojnega nacionalnega organa (v nadaljnjem besedilu: PNO), enotne kontaktne točke, nacionalnega okvira za obvladovanje kibernetskih kriz in skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT). Za slednje določa zahteve in tehnične zmogljivosti ter njihove naloge in sodelovanje z deležniki zasebnega sektorja. To poglavje vsebuje tudi določbe o usklajenem razkrivanju ranljivosti in evropski podatkovni zbirki ranljivosti, sodelovanju na nacionalni ravni ter o. medsebojnem strokovnem pregledu.

K 8. členu

Predlog člena prenaša določbo 7. člena Direktive 2022/2555, ki določa, da vsaka država članica sprejme nacionalno strategijo, v kateri so opredeljeni strateški cilji, potrebna sredstva za dosego teh ciljev ter ustrezni ukrepi politike in regulativni ukrepi za doseganje in ohranjanje visoke ravni kibernetske varnosti. Glede na navedeno so v predlogu člena določeni obveznost sprejetja strategije kibernetske varnosti, njena vsebina, namen in cilj. Elementi vsebine, ki jih mora strategija vsebovati, so taksativno našteti. Republika Slovenija že ima izdelano Strategijo kibernetske varnosti Republike Slovenije, ki jo je vlada sprejela 25. februarja 2016, bo pa po sprejetju predlaganega zakona to strategijo treba prilagoditi njegovim zahtevam. Tudi sicer je v predlogu zakona v prehodni določbi tretjega odstavka 59. člena predviden časovni okvir za sprejem strategije oziroma prilagoditev strategije določbam tega zakona (najkasneje v roku enega leta od uveljavitve tega zakona).

K 9. členu

Glede na zahteve 8. člena Direktive 2022/2555 je v predlaganem členu določen PNO.
V prvem odstavku je določeno, da je PNO Urad Vlade Republike Slovenije za informacijsko varnost.
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 čemer gre za naloge, ki izhajajo tako iz Direktive 2022/2555 kot tudi takšne, ki so nacionalne narave. Pri tem na primer PNO koordinira delovanje nacionalnega sistema informacijske varnosti, razvija zmogljivosti za izvajanje kibernetske obrambe, vsem zavezancem pri izvajanju njihovih nalog nudi strokovno podporo, sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti in izvaja naloge mednarodnega sodelovanja.

K 10. členu

Glede na zahteve 8. člena Direktive 2022/2555 je v predlaganem členu s prvim odstavkom določena enotna kontna točka, ki je PNO. , Po drugem odstavku enotna kontaktna točka (PNO) zagotavlja čezmejno sodelovanja z ustreznimi organi drugih držav članic Evropske unije in, kadar je to ustrezno, Evropsko komisijo in ENISA ter medsektorsko sodelovanje z drugimi pristojnimi organi za kibernetsko varnost v Republiki Sloveniji skladno s področnimi predpisi. PNO po tretjem odstavku o določitvi enotne kontaktne točke, njenih nalogah in ob vsakokratnih spremembah o tem brez nepotrebnega odlašanja uradno obvesti Evropsko komisijo.

K 11. členu

Določbe 9. člena Direktive 2022/2555 zahtevajo, da vsaka država članica imenuje ali ustanovi enega ali več pristojnih organov, odgovornih za obvladovanje kibernetskih incidentov velikih razsežnosti in kibernetikih kriz (v nadaljnjem besedilu: organi za obvladovanje kibernetskih kriz).

V prvem odstavku predlaganega člena je določeno, da je organ za obvladovanje kibernetskih kriz Urad Vlade Republike Slovenije za informacijsko varnost, ki sodeluje v Evropski mreži organizacij za zvezo za kibernetske krize (v nadaljnjem besedilu: mreža EU-CyCLONe).
Drugi odstavek določa, da organ za obvladovanje kibernetskih kriz izdela nacionalni načrt odzivanja na kibernetske incidente, kibernetske incidente velikih razsežnosti in krize.
Tretji odstavek pa določa vsebino omenjenega načrta, ki ga sprejme vlada.
V četrtem odstavku je določen postopek odzivanja na kibernetske krize ter obveznost obveščanja ob zaznavi kibernetskih incidentov, za katere organ za obvladovanje kibernetskih kriz ocenjuje, da lahko povzročijo kibernetsko krizo.
Peti odstavek pooblašča vlado, da na predlog SNAV lahko sprejme odločitev o vključitvi drugih državnih zmogljivosti v obvladovanje krize, razglasi krizo ter o potrebi sprejme odločitev o izvajanju kriznega upravljanja in vodenja v kompleksni krizi.
Šesti odstavek uvaja dolžnost obveščanja Evropske komisije o imenovanju organa za obvladovanje kibernetskih kriz in vsakokratnih spremembah o tem, pri čemer je PNO tisti, ki obvešča. Prav tako PNO Evropski komisiji in mreži EU-CyCLONE predloži ustrezne informacije o sprejetju nacionalnega načrta odzivanja v zvezi z zahtevami iz tretjega odstavka predlaganega člena, pri čemer je določena varovalka glede izključitve informacij, katerih razkritje bi bilo v nasprotju z interesi nacionalne varnosti, javne varnosti ali obrambe Republike Slovenije.
Sedmi odstavek pa za primer, da je v zvezi z izvajanjem tega člena potrebno tudi obveščanje javnosti, glede na občutljivost zadevnih informacij predvideva, da pristojni nacionalni organ skupaj s službo vlade, pristojno za komuniciranje z javnostjo, pripravi sporočilo za javno objavo, ki ga mediji smejo objaviti le v nespremenjeni obliki.

K 12. členu

V tem predlogu člena gre za prenos določb 10. Direktive 2022/2555 (skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT), ki se pri nekaterih svojih določbah sklicuje tudi na prvi odstavek 11 člena (Zahteve, tehnične zmogljivosti in naloge skupin CSIRT), na 19. člen (Medsebojni strokovni pregledi) . in na 29. člen (Dogovori o izmenjavi o kibernetski varnosti) Direktive 2022/2555, kar je bilo upoštevano tudi v predlaganem členu, ki se na posamičnih mestih sklicuje na druge določbe predlaganega zakona, ki ustrezajo prenosu prej navedenih določb Direktive 2022/2555
V prvem odstavku predloga tega člena sta najprej določeni skupini CSIRT, ki sta CSIRT SI-CERT ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije ter CSIRT državne uprave (pojasnjujemo, da gre za CSIRT organov državne uprave po ZInfV), ki deluje kot notranja organizacijska enota SIGOV-CERT pri PNO. Skupini CSIRT delujeta kot odzivna centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Posledično opravljata koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah, ter izdajata opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih.
V drugem in tretjem odstavku je določena pristojnost posamezne skupine CSIRT za tam navedene skupine zavezanih subjektov.
Od petega do desetega odstavka predloga je urejeno področje izmenjave informacij, medsebojnega in mednarodnega sodelovanja.
Enajsti odstavek uvaja dolžnost obveščanja Evropske komisije o identiteti skupin CSIRT iz prvega odstavka tega člena ter njihovih nalogah iz drugega in tretjega odstavka tega člena, kot tudi o vsakokratnih spremembah o tem, pri čemer je PNO tisti, ki obvešča. Prav tako PNO obvesti Evropsko komisijo tudi o identiteti skupine CSIRT, ki je imenovana za koordinatorja iz prvega odstavka 16. člena tega zakona (usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti).

K 13. členu

OBRAZLOŽITVE K OSNUTKU PREDLOGA

V tem predlogu člena gre za prenos določbe prvega odstavka 11. člena Direktive 2022/2555.Predlog člena tako ureja zahteve in tehnične zmogljivosti, ki jih morata izpolnjevati skupini CSIRT.

K 14. členu

V tem predlogu člena gre za prenos določbe tretjega odstavka 11. člena Direktive 2022/2555, ki določa naloge skupin CSIRT.
Prvi odstavek predlaganega člena taksativno našteje naloge obeh skupin CSIRT, ki jih morata izvajati.
V drugem odstavku predlog določa pristojnost, da skupini CSIRT lahko izvajata proaktivno in nevsiljivo pregledovanje javno dostopnih omrežnih in informacijskih sistemov bistvenih in pomembnih subjektov, za katere je pristojna.
S predlaganim tretjim odstavkom se skupinama CSIRT omogoča, da lahko pri izvajanju nalog iz prvega odstavka predlaganega člena prednostno razvrstita nekatere naloge na podlagi pristopa, ki temelji na tveganjih.
V četrtem odstavku predloga je navedena obveznost izdelave tedenskega in četrtletnega poročila o izvajanju svojih nalog, ki ga morata skupini CSIRT posredovati PNO.
V petem odstavku predloga je predvidena obveznost nacionalne narave, da skupina CSIRT obvesti PNO o lastnem incidentu, ki bi lahko vplival ali vpliva na delovanje in razpoložljivost njihovih storitev, ki jih nudijo zavezancem in prostovoljnim priglasiteljem.
Po predlaganem šestem odstavku, ki je nacionalne narave, skupina CSIRT v skladu z usmeritvami pristojnega nacionalnega organa v primeru razglasitve ocene ogroženosti visoko ali kritično izda varnostno obvestilo ali navodilo v skladu s petim in šestim odstavkom 33. člena tega zakona.
Tudi predlagana sedmi in osmi odstavek sta nacionalne narave in nudita dodatno potrebna pooblastila CSIRT-u državne uprave, pri čemer določbi vsebinsko ustrezata obstoječim določbam tretjega in četrtega odstavka 29. člena veljavnega ZInfV. Po navedenih določbah ZInfV je CSIRT organov državne uprave že doslej in z enakimi nameni, kot je to ponovno določeno za CSIRT državne uprave v tem predlogu, pooblaščen za neposredni, nujni in sorazmerni vpogled v delovanje informacijske infrastrukture centralnega informacijsko-komunikacijskega sistema, upravljavec centralnega informacijsko-komunikacijskega sistema pa mu mora to omogočiti kot tudi, da upravljavcu centralnega informacijsko-komunikacijskega sistema oziroma povezanim subjektom odredi ustrezne, nujne in sorazmerne ukrepe, ki jih morajo ti nemudoma oziroma v postavljenem roku izvesti v svojem informacijsko-komunikacijskem sistemu.
Deveti odstavek predloga določa, da skupini CSIRT lahko izvajata tudi programe ozaveščanja v skladu s Strategijo kibernetske varnosti.

K 15. členu

V tem predlogu člena gre za prenos določbe četrtega in petega odstavka 11. člena Direktive 2022/2555, ki za dosego ciljev določa vzpostavitev sodelovanje z ustreznimi deležniki iz zasebnega sektorja.
V prvem odstavku predloga je predvideno sodelovanje skupin CSIRT z ustreznimi deležniki iz zasebnega sektorja.
Drugi odstavek predloga pa določa način in namen sodelovanja ter taksonomijo.
Tretji odstavek predloga pa nalaga skupini CSIRT, ki zazna ranljivost informacijsko-komunikacijskega sistema, da mora o tem brez nepotrebnega odlašanja obvestiti skrbnika sistema.

K 16. členu

V tem predlogu člena gre za prenos določbe 12. člena Direktive 2022/2555, ki vpeljuje rešitev usklajenega razkrivanja ranljivosti in evropsko podatkovno zbirko ranljivosti.
Prvi odstavek predloga določa, da je koordinator za usklajeno razkrivanje ranljivosti v Republiki Sloveniji (v nadaljnjem besedilu koordinator) skupina CSIRT SI-CERT. Koordinator olajšuje sodelovanje med fizično ali pravno osebo, ki poroča o ranljivostih, in proizvajalcem ali ponudnikom proizvodov IKT ali storitev IKT, ki naj bi zajemali ranljivost, in sicer na pobudo katere koli stranke. Pojasnjujemo, da SI-CERT omenjeno nalogo že samoiniciativno opravlja od oktobra 2023.

Drugi odstavek predloga določa naloge koordinatorja. Tretji odstavek predloga omogoča, da fizične ali pravne osebe lahko koordinatorju o ranljivostih poročajo anonimno. Koordinator po potrebi sodeluje z drugimi skupinami CSIRT, ki so imenovane za koordinatorke v okviru mreže skupin CSIRT. Četrti odstavek predloga nalaga koordinatorju sodelovanje z ENISO, ki vodi evropsko podatkovno zbirko ranljivosti. Pet, šesti, sedmi in osmi odstavek predloga določa vzpostavitev nacionalne zbirke ranljivosti ter sodelovanje med koordinatorjem in pristojnim nacionalnim organom.

K 17. členu

V tem predlogu člena gre za prenos določbe 13. člena Direktive 2022/2555 o sodelovanju na nacionalni ravni.
Prvi odstavek predloga za zagotovitev učinkovitega opravljanja nalog in obveznosti pristojnega nacionalnega organa, enotne kontaktne točke in skupin CSIRT določa, da se vzpostavi ustrezno sodelovanje na nacionalni ravni. Oblike sodelovanja se izvajajona način, da medsebojno sodelujejo pri izpolnjevanju obveznosti; da sodelujejo z organi kazenskega pregona, Informacijskim pooblaščencem, Javno agencijo za civilno letalstvo Republike Slovenije, Inšpekcijo za informacijsko družbo, Banko Slovenije, Agencijo za komunikacijska omrežja in storitve Republike Slovenije in pristojnim organom iz zakona, ki ureja kritično infrastrukturo ter pristojnimi organi oziroma sektorskimi regulatorji iz drugih področnih zakonov iz področij, ki jim pripadajo zavezanci iz 6. člena tega zakona; da redno sodelujejo s pristojnim organom iz zakona, ki ureja kritično infrastrukturo in si izmenjujejo informacije o identifikaciji kritičnih subjektov, o tveganjih, kibernetskih grožnjah in incidentih, pa tudi o nekibernetskih tveganjih, grožnjah in incidentih, ki vplivajo na bistvene subjekte, ki so opredeljeni kot kritični subjekti na podlagi zakona, ki ureja kritično infrastrukturo, ter o ukrepih, sprejetih v odziv na takšna tveganja, grožnje in incidente ter redno izmenjujejo informacije, tudi o relevantnih incidentih in kibernetskih grožnjah z Inšpekcijo za informacijsko družbo, Banko Slovenije, Javno agencijo za civilno letalstvo Republike Slovenije in Agencijo za komunikacijska omrežja in storitve Republike Slovenije.
Drugi odstavek predloga določa obveznost medsebojne izmenjava informacij o incidentih, kibernetskih grožnjah in skorajšnjih incidentih. Za ta namen PNO vzpostavi digitalno platformo.
Tretji odstavek predloga pa določa, da za potrebe nacionalnega sistema za zagotavljanje informacijske varnosti lahko pristojni nacionalni organ in skupine CSIRT sodelujejo s subjekti v javni upravi, gospodarstvu, z raziskovalno-razvojnimi organizacijami, znanstvenimi institucijami, interesnimi združenji in posamezniki. Gre za določbo, ki jo ohranjamo iz obstoječega Zakona o informacijski varnosti (30. člen).

K 18. členu

V tem predlogu člena gre za prenos določbe 19. člena Direktive 2022/2555 o medsebojnih strokovnih pregledih.
Prvi odstavek predloga določa, da PNO lahko odloči, da z namenom učenja iz skupnih izkušenj, okrepitve medsebojnega zaupanja, doseganja visoke skupne ravni kibernetske varnosti ter okrepitve zmogljivosti in politike na področju kibernetske varnosti, pristopi k medsebojnim strokovnim pregledom, ki jih izvajajo imenovani strokovnjaki s področja kibernetske varnosti drugih držav članic Evropske unije. Evropske komisija in ENISA sodelujeta v medsebojnih strokovnih pregledih kot opazovalki. Drugi odstavek predloga določa področja medsebojnih strokovnih pregledov. Tretji odstavek predloga določa, da se uporablja metodologija, ki jo pripravi Skupina za sodelovanje s pomočjo Evropske komisije in ENISA ter po potrebi mreža skupin CSIRT. Četrti odstavek predloga določa postopke pred začetkom medsebojnega strokovnega pregleda. PNO lahko v skladu s petim odstavkom predloga pred začetkom medsebojnega strokovnega pregleda izvede samooceno vidikov, ki bodo pregledani. Šesti odstavek predloga določa obseg medsebojnih strokovnih pregledov, med tem ko sedmi odstavek predloga omejuje uporabo informacij pridobljenih v okviru medsebojnega strokovnega pregleda. Osmi odstavek predlog določa način izbire strokovnjakov. PNO lahko v skladu z devetim odstavkom predloga lahko

nasprotuje imenovanju posameznih strokovnjakov. V skladu z desetim odstavkom predloga strokovnjaki za kibernetsko varnost, ki sodelujejo v medsebojnih strokovnih pregledih, pripravijo poročila o ugotovitvah. PNO lahko v skladu z enajstim odstavkom predloga predloži pripombe na osnutek poročila, ter se lahko odloči, da naredi poročilo javno ali njegovo redigirano različico javno dostopno.

IV. Ukrepi za obvladovanje tveganj in priglasitve incidentov

Poglavje vsebuje določbe glede upravljanja, ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, dnevniških zapisov, obveze posredovanja podatkov in informacij, certifikacijske sheme za kibernetsko varnost, standardizacije in obveznosti priglašanja in obveščanja. Določa tudi postopek priglasitve pomembnih incidentov.

K 19. členu

V tem predlogu člena gre za prenos določbe 20. člena Direktive 2022/2555 o upravljanju.
Prvi odstavek predloga določa, da so odgovorne osebe pravnih oseb oziroma člani poslovodnih organov bistvenega ali pomembnega subjekta, odgovorne za izvajanje ukrepov za obvladovanje tveganj za kibernetsko varnost v skladu z določbami tega zakona. Drugi odstavek predloga določa, da morajo odgovorne osebe odobriti ukrepe za obvladovanje tveganj za kibernetsko varnost, ki jih subjekt izvaja zaradi izpolnjevanja obveznosti, določenih s tem zakonom in nadzirati njihovo izvajanje. Tretji odstavek predloga pa nalaga odgovorni osebi, da se mora izobraževati oziroma usposabljati na področju obvladovanja tveganj kibernetske varnosti in njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt. Odgovorne osebe po predlogu četrtega odstavka morajo zagotoviti redno usposabljanje zaposlenim, da pridobijo dovolj znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt. Peti odstavek predloga določa, da mora odgovorna oseba zagotoviti, da imajo vsi skrbniki informacijsko komunikacijskih sistemov zavezanca obveznost rednega letnega usposabljanja, da pridobijo in ohranijo raven znanj in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja ta subjekt.

K 20. členu

V tem predlogu člena gre za prenos določb 21. in 22. člena Direktive 2022/2555, ki določata ukrepe za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov oziroma usklajeno oceno tveganja za varnost na ravni Unije za kritične dobavne verige.
Prvi odstavek predloga določa, da morajo bistveni in pomembni subjekti sprejeti ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih ti subjekti uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve. Drugi odstavek predloga določa na kakšen način bistveni in pomembni subjekti izvedejo oceno tveganja. Tretji odstavek predloga določa, da morajo zavezanci upoštevajo vse nevarnosti, katerega namen je zaščititi omrežne in informacijske sisteme ter njihovo fizično okolje pred incidenti ter minimalni obseg ukrepov.
Četrti odstavek predloga določa, da morajo bistveni in pomembni subjekti pri preučevanju ustreznih ukrepov upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki. Peti odstavek predloga pa določa, da morajo preverjati izvajanje ukrepov. Če pri tem ugotovijo, da ne izpolnjujejo vseh ukrepov ali pa so ti neustrezno izvajani, morajo brez nepotrebnega odlašanja sprejeti vse potrebne, ustrezne in sorazmerne popravne ukrepe. Šesti odstavek predloga določa, da ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki

spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja in ponudniki storitev zaupanja pri sprejemu ukrepov upoštevajo izvedbene akte Evropske komisije. Ostali zavezanci v skladu s predlogom sedmega člena upoštevajo morebitne izvedbene akte Evropske komisije. Predlog osmega odstavka pa daje pristojnost vladi, da lahko podrobneje določi način izvajanja obveznosti iz tega člena in minimalni obseg varnostnih ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, v kolikor niso zajeti v dokumentih Evropske komisije.
V predlogu devetega odstavka se uvaja prepoved, po kateri bistveni in pomembni subjekti ne smejo uporabljati informacijsko-komunikacijskih rešitev, ki imajo aktivno izkoriščane ranljivosti, brez dodatne izvedbe ocene tveganja in kjer je to glede na oceno tveganja primerno, ustreznih popravljalnih ukrepov, ki znižajo stopnjo tveganja na sprejemljivo raven. Predloga desetega odstavka nalaga skupinam CSIRT, da zavezance obvestita o ranljivostih informacijsko-komunikacijskih rešitev, ki jih uporabljajo zavezanci, za katere sta pristojni in s katerimi sta seznanjeni, če jih štejeta za kritične, lahko pa tudi za visoko pomembne, v skladu z mednarodno sprejetimi praksami za določanje ranljivosti.
Predlagani enajsti odstavke je nacionalne narave in vsebinsko ohranja določbo četrtega odstavka 11. člena ZInfV, le da posodablja besedilo v skladu s predlaganim zakonom. Če torej bistveni ali pomembni subjekti za opravljanje svoje dejavnosti črpajo vhodne podatke in informacije iz ključnih delov nacionalnovarnostnega sistema, v skladu s predlagano določbo vzpostavijo vse potrebne varnostne zahteve ob soglasju pristojnega ministrstva ali vladne službe za posamezni ključni del nacionalnovarnostnega sistema.

K 21. členu

V tem predlogu člena gre za nacionalno določbo, ki določa hrambo dnevniških zapisov. Gre za rešitev iz obstoječega zakona, ki se je izkazala kot pomembna za dvig kibernetske varnosti zavezancev.
Prvi odstavek predloga določa, da zavezanci za namen obvladovanja in preprečevanja incidentov, v skladu s politikami o analizi tveganja in varnosti informacijskih sistemov in ob upoštevanju stanja tehnike zagotovijo tudi ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja, za obdobje šestih mesecev, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov.
Drugi odstavek predloga, določa, da se ohranjanje dnevniških zapisov zagotavlja na ozemlju Republike Slovenije, razen za področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, glede katerih se lahko zagotavlja na ozemlju Evropske unije.
Tretji odstavek predloga določa način hrambe dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja
razpoložljivost v primeru incidentov.

K 22. členu

V tem predlogu člena gre za nacionalno določbo, ki določa obveza posredovanja podatkov in informacij). Gre za rešitev iz obstoječega zakona, ki se je izkazala kot pomembna za dvig kibernetske varnosti zavezancev.
Prvi odstavek predloga določa, da morajo bistveni in pomembni subjekti pristojnemu nacionalnemu organi na podlagi pisne zahteve posredovati podatke in informacije brez nepotrebnega odlašanja. Gre za podatke in informacije, ki jih pristojni nacionalni organ potrebuje za izvajanje svojih pristojnosti po tem zakonu.
Drugi odstavek predloga pa ureja obseg zahteve do podatkov in informacij. Le-ta mora biti sorazmerni namenu, za katerega bodo uporabljeni. Pristojni nacionalni organ mora v zahtevi navesti namen uporabe zahtevanih podatkov in informacij.

K 23. členu

V tem predlogu člena gre za prenos določbe 24. Direktive 2022/2555, ki določa certifikacijske sheme za kibernetsko varnost.
Prvi odstavek predloga določa, da bistveni in pomembni subjekti zaradi zagotavljanja višje ravni kibernetske varnosti z namenom zagotovitve skladnosti z nekaterimi zahtevami iz 20. člena tega zakona prednostno uporabljajo proizvode IKT, storitve IKT in postopke IKT ter so jih razvili bistveni ali pomembni subjekti ali ki so bili kupljeni pri tretjih straneh in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi člena 49 Uredbe (EU) 2019/881[10] oziroma so prestali presojo s strani organov za ugotavljanje skladnosti, ki so bili akreditirani in po potrebi pooblaščeni, da izvajajo presojo za posamezno evropsko certifikacijsko shemo
Drugi odstavek predloga določa, da pristojni nacionalni organ spodbuja bistvene in pomembne subjekte, da pri izvajanju ukrepov iz 20. člena tega zakona, kjer je to možno in primerno, uporabljajo kvalificirane storitve zaupanja .
Tretji odstavek predloga določa, da bistveni in pomembni subjekti iz kategorij, ki jih lahko določi Evropska komisija z delegiranim aktom, morajo za obvladovanje tveganj za kibernetsko varnost uporabljati v njem določene certificirane proizvode IKT, storitve IKT in procese IKT ali pridobiti certifikat na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49 Uredbe (EU) 2019/881.

K 24. členu

V tem predlogu člena gre za prenos določbe 25. člena Direktive 2022/2555, ki določa standardizacijo. Gre za rešitev, ki je že uveljavljena z 19. členom obstoječega zakona.
Prvi odstavek predloga določa, da bistveni in pomembni subjekti zaradi zagotovitve skladnega izvajanja ukrepov iz 20. člena tega zakona v čim večji meri uporabljajo evropske in mednarodne standarde in tehnične specifikacije, ki obravnavajo varnost omrežnih in informacijskih sistemov. Pri tem upoštevajo tudi nasvete in smernice ENISA. Drugi odstavek predloga določa nalogo pristojnemu nacionalnemu organu, da na svoji spletni strani objavlja ustrezne informacije ter osvešča zavezance k njihovi uporabi.

K 25. členu

V tem predlogu člena gre za prenos določb prvega, drugega in tretjega odstavka 23.člena Direktive 2022/2555, ki določa obveznost priglašanja in obveščanja.
Prvi odstavek predloga določa, da bistveni in pomembni subjekti pristojni skupini CSIRT brez nepotrebnega odlašanja priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev. Odstavek tudi definira kaj se šteje za pomemben incident.
Drugi odstavek predloga določa, da se upoštevajo morebitni izvedbeni akti Evropske komisije, s katerimi ta podrobneje določi vrsto informacij, obliko in postopek priglasitve ter prostovoljne priglasitve in obvestila.
Tretji odstavek predloga določa, da ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, kot tudi ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja, pri priglašanju upoštevajo izvedbene akte Evropske komisije, v katerih so zanje podrobneje določeni primeri, ko se incident šteje za pomembnega. Četrti odstavek predloga za ostale bistvene in pomembne subjekte določa, da upoštevajo morebitne izvedbene akte Evropske komisije. Če Evropska komisija takšnih izvedbenih aktov ne sprejme, se za te subjekte upošteva metodologija za določitev pomembnosti incidenta, kot je opredeljena v nacionalnem načrtu odzivanja.

[10] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, z dne 7. 6. 2019, str. 15) (v nadaljnjem besedilu Uredbe (EU) 2019/881).

Peti odstavek predloga nalaga katere informacije morajo posredovati bistveni in pomembni subjekti pristojni skupini CSIRT. Določa tudi postopek posredovanja informacije enotni kontaktni točki.
Šesti odstavek predloga obvezuje bistvene in pomembne subjekte, da brez nepotrebnega odlašanja uradno obvestijo prejemnike svojih storitev o pomembnih incidentih, ki bodo verjetno negativno vplivali na zagotavljanje teh storitev.
Sedmi odstavek predloga pa bistvene in pomembne subjekte zavezuje, da brez nepotrebnega odlašanja prejemnikom svojih storitev, ki bi jih pomembna kibernetska grožnja lahko prizadela, sporočijo vse ukrepe ali sredstva, ki jih lahko ti prejemniki sprejmejo v odziv na to grožnjo.

K 26. členu

V tem predlogu člena gre za prenos določb četrtega odstavka 23.člena Direktive 2022/2555, ki določa obveznost poročanja oziroma postopek priglasitve pomembnih incidentov. Prenašajo se tudi tretji in šesti odstavek 13. člena Direktive 2022/2555
Prvi odstavek predloga določa kaj morajo bistveni in pomembni subjekti za namen priglasitve pomembnih incidentov predložiti in poročati pristojni skupini CSIRT.
Drugi odstavek predloga določa posebno zahtevo za ponudnike storitev zaupanja v zvezi s pomembnimi incidenti, ki vplivajo na zagotavljanje njegovih storitev.
Tretji odstavek predloga nalaga postopek odzivanja skupine CSIRT po prejeti priglasitvi, ki vključuje odgovor priglasitvenemu subjektu, seznanitev PNO ter usmeritve o poročanju organom kazenskega pregona.
Četrti odstavek predloga določa postopek v primeru pomembnega čezmejnega ali medsektorskega pomembnega incidenta. Pri obveščanju prek enotne kontaktne točke v skladu s pravom Evropske unije ali pravom Republike Slovenije zaščiti varnost in poslovne interese zavezanca ter zaupnost predloženih informacij, ki jih slednji zagotovi v svoji priglasitvi.
Peti odstavek predloga določa, da enotna kontaktna točka vsake tri mesece predloži zbirno poročilo o prejetih priglasitvah na ENISA.
Šesti odstavek predloga ureja področje ozaveščanja javnosti kadar je potrebno za preprečitev pomembnega incidenta ali obravnavo pomembnega incidenta, ki je v teku, ali kadar je razkritje pomembnega incidenta kako drugače v javnem interesu.
Sedmi odstavek predloga določa postopek, ki ga izvede PNO, ko je preko enotne kontaktne točke obveščen o pomembnem čezmejnem ali medsektorsko pomembnem incidentu, ki ima vpliv tudi v Republiki Sloveniji.
Osmi odstavek predloga določa, da mora PNO zagotoviti pristojnim organom iz zakona, ki ureja kritično infrastrukturo, informacije o pomembnih incidentih, incidentih, kibernetskih grožnjah in skorajšnjih incidentih, ki so jih priglasili bistveni subjekti, ki so identificirani kot kritični subjekti na podlagi predpisov, ki urejajo kritično infrastrukturo.
Deveti odstavek predloga določa, da mora pristojna skupina CSIRT o pomembnem incidentu nemudoma obvestiti PNO, ki vodi seznam pomembnih incidentov. S tem se prenaša tudi tretji odstavek 13. člena Direktive 2022/2555, ker je PNO hkrati enotna kontaktna točka. Pristojni nacionalni organ o incidentu, ki bi lahko imel večji medsektorski vpliv oziroma bi lahko ob daljšem trajanju povzročil slabšanje stabilnosti nacionalne varnosti Republike Slovenije, obvesti Nacionalni center za krizno upravljanje, lahko pa obvesti tudi druge pristojne organe, s katerimi sodeluje na nacionalni ravni v skladu s 17. členom tega zakona.
Deseti odstavek predloga predvideva vzpostavitev namenske digitalne platforme za priglasitev, ki jo vzpostavijo skupine CSIRT in pristojni nacionalni organ. Gre za prenos šestega odstavka 13. člena Direktive 2022/2555.
Enajsti odstavek predloga ohranja ureditev iz obstoječega zakona, ki ureja področje informacijske varnosti, ki določa, da PNO vodi (1) skupen seznam pomembnih incidentov, ki vsebuje podatke iz končnih poročil o incidentih iz tega člena in(2) seznam omrežnih in informacijskih sistemov, delov

omrežja in digitalnih oziroma elektronskih komunikacijskih storitev zavezancev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

V. Ukrepi za obvladovanje tveganj in priglasitve incidentov

Poglavje vsebuje določbe glede pristojnosti in teritorialnost, zbiranja informacij za register ponudnikov storitev pri ENISA in podatkovne zbirke o registraciji domenskih imen.

K 27. členu

V tem predlogu člena gre za prenos določb 26. člena Direktive 2022/2555, ki določa pristojnost in teritorialnost.
Prvi odstavek predloga določa, da zavezanci na podlagi tega zakona spadajo v pristojnost pristojne skupine CSIRT, ki ji priglašajo incidente, če jih je ustanovila Republika Slovenija ali imajo sedež v Republiki Sloveniji. Izjemi se nanašata na (1) ponudnike javnih elektronskih komunikacijskih omrežij ali ponudnike javno dostopnih elektronskih komunikacijskih storitev šteje, da spadajo v pristojnost države članice Evropske unije, v kateri zagotavljajo svoje storitve in (2) ponudnike storitev DNS, registre TLD imen, subjekte, ki opravljajo storitve registracije domenskih imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnih centrov, ponudnike omrežij za dostavo vsebine, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev ter ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja šteje, da spadajo v pristojnost države članice, v kateri imajo glavni sedež v Evropski uniji v skladu z drugim odstavkom tega člena. Za slednje drugi odstavek predloga določa, da imajo glavni sedež v Evropski uniji v državi članici Evropske unije, kjer se sprejme večina odločitev v zvezi z ukrepi za obvladovanje tveganj za kibernetsko varnost. Če te države članice Evropske unije ni mogoče določiti ali če se te odločitve ne sprejemajo v Evropski uniji, se šteje, da je glavni sedež v državi članici Evropske unije, kjer se izvajajo operacije v zvezi s kibernetsko varnostjo. Če te države članice Evropske unije ni mogoče določiti, se šteje, da je glavni sedež v državi članici, kjer ima zadevni subjekt sedež z največjim številom zaposlenih v Evropski uniji.
Tretji odstavek predloga uvaja rešitev, za subjekt, ki nima sedeža v Evropski uniji, v njej pa zagotavlja takšne storitve, določi sedež svojega predstavnika za Evropsko unijo v Republiki Sloveniji, kjer tudi zagotavlja takšne storitve, spada v pristojnost pristojnega nacionalnega organa in pristojne skupine CSIRT. Predstavnik zastopa subjekt v zvezi z obveznostmi na podlagi tega zakona.
Četrti odstavek predloga določa postopek, subjekt ni imenoval predstavnika v Evropski uniji opravlja pa storitve v Republiki Slovenije.
Peti odstavek predloga določa postopek, če PNO organ prejme zahtevek za medsebojno pomoč na podlagi 49. člena tega zakona v zvezi s subjektom iz druge alineje prvega odstavka tega člena.

K 28. členu

V tem predlogu člena gre za prenos določb 27. člena Direktive 2022/2555, ki določa register subjektov oziroma zbiranje informacij za register ponudnikov storitev pri ENISA.
Prvi odstavek predloga določa, da subjekti, ki sodijo v pristojnost PNO morajo podati informacije (1) ime subjekta; (2) ustrezni sektor, podsektor in vrsto subjekta iz Priloge I ali II, kadar je to ustrezno; (3) naslov njegovega glavnega sedeža in njegovih drugih zakonitih sedežev v Evropski uniji ali, če nima sedeža v Evropski uniji, njegovega predstavnika, imenovanega v skladu s tretjim odstavkom 27. člena tega zakona; (4) posodobljene kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami subjekta in po potrebi njegovega zastopnika, imenovanega v skladu s tretjim odstavkom 27. člena tega zakona; (5) države članice, v katerih subjekt opravlja storitve, ter (6) bloke subjektu dodeljenih številk avtonomnih sistemov in javnih naslovov IP.
Drugi odstavek predloga določa, da morajo subjekti PNO obvestiti o vsaki spremembi informacij iz prvega odstavka.
Tretji odstavek predloga določa, da subjekti predložijo informacije PNO prek mehanizma za samoregistracijo zavezancev iz prvega odstavka 7. člena predloga zakona.

Četrti odstavek predloga določa postopek posredovanja zbranih informacij ENISI, ki vzpostavitvi in vzdržuje registra ponudnikov storitev iz prvega odstavka tega člena.

K 29. členu

V tem predlogu člena gre za prenos določb 28. člena Direktive 2022/2555, ki določa podatkovno zbirko o registraciji domenskih imen.
Prvi odstavek predloga določa, da registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen zaradi zagotovitve varnosti, stabilnosti in odpornosti DNS z ustrezno skrbnostjo zbirajo ter vzdržujejo točne in popolne podatke o registraciji domenskih imen v posebni podatkovni zbirki, pri čemer za zbrane osebne podatke upoštevajo predpise s področja varstva osebnih podatkov.
Drugi odstavek predloga določa, da morajo podatkovna zbirke vsebovati potrebne informacije o registraciji domenskih imen, ki vsebujejo potrebne informacije za identifikacijo imetnikov domenskih imen in kontaktnih točk, ki upravljajo domenska imena v okviru vrhnjih domenskih imen, in navezavo stika z njimi.
Tretji odstavek predloga nalaga vzpostavitev politike in postopke, vključno s postopki preverjanja, ki zagotavljajo, da podatkovne zbirke iz prvega odstavka tega člena vključujejo točne in popolne informacije. Te politike in postopki morajo biti javno dostopni.
Četrti odstavek predloga določa, da subjekti po registraciji domenskega imena brez nepotrebnega odlašanja podatke o registraciji, ki niso osebni podatki, naredijo javno dostopne.
Peti odstavek določa postopek dostopa do podatkov o registraciji posameznih domenskih imen na podlagi zakonitih in ustrezno utemeljenih zahtevkov oseb, ki imajo upravičen razlog za dostop, v skladu s predpisu s področja varstva osebnih podatkov.
Šesti odstavek predloga pa uvaja varovalo pred podvajanjem zbiranja podatkov o registraciji domenskih imen.

VI. Izmenjava informacij

Poglavje vsebuje določbi glede dogovorov o izmenjavi informacij o kibernetski varnosti in prostovoljne priglasitve.

K 30. členu

V tem predlogu člena gre za prenos določb 29. člena Direktive 2022/2555, ki določa dogovore o izmenjavi informacij o kibernetski varnost.
Prvi odstavek predloga določa, da si zavezanci na podlagi tega zakona ter, kadar je to ustrezno, tudi drugi subjekti, si lahko prostovoljno izmenjujejo ustrezne informacije o kibernetski varnosti, vključno z informacijami, ki se nanašajo na kibernetske grožnje, skorajšnje incidente, ranljivosti, tehnike in postopke, kazalnike ogroženosti, sovražne taktike, specifične informacije o grožnji in akterju, opozorila glede kibernetske varnosti in priporočila glede konfiguracije orodij za kibernetsko varnost za zaznavo zlonamernih kibernetskih aktivnosti.
Drugi odstavek predloga določa, da izmenjava informacij poteka v skupnostih zavezancev ter, kadar je to ustrezno, z njihovimi dobavitelji ali ponudniki storitev. Taka izmenjava se izvaja na podlagi dogovorov o izmenjavi informacij o kibernetski varnosti, ob upoštevanju morebitne občutljive narave informacij, ki se izmenjujejo. Pri sklenitvi dogovorov o izmenjavi informacij se kar najbolj upoštevajo dobre prakse in smernice ENISA.
Tretji odstavek predloga nalaga PNO, da spodbuja sklenitev dogovorov o izmenjavi informacij o kibernetski varnosti iz prejšnjega odstavka, ki lahko vključujejo operativne elemente, vključno glede uporabe namenskih digitalnih platform in orodij za avtomatizacijo ter vsebine in pogoje za dogovore o izmenjavi informacij.
Četrti odstavek predloga nalaga bistvenim in pomembnim subjektom, da morajo obvestiti PNO in za njih pristojno skupino CSIRT o svojem sodelovanju pri dogovorih o izmenjavi informacij o kibernetski varnost.
Peti odstavek predloga ureja instrument, da na zaprosilo zavezancev iz tega zakona PNO ali skupini CSIRT lahko sodelujejo pri posamičnem dogovoru iz prejšnjega odstavka in pri tem določijo pogoje glede informaciji, ki jih dajo na voljo.

K 31. členu

V tem predlogu člena gre za prenos določb 30. člena Direktive 2022/2555, ki določa dogovore o prostovoljni priglasitvi ustreznih informacij.
Prvi odstavek predloga zavezanim subjektom poleg obvezne priglasitve skupinam CSIRT prostovoljno priglasijo incidente, kibernetske grožnje in skorajšnje incidente in jim predložijo ustrezne informacije.
Drugi odstavek predloga omogoča, da subjekti, ki niso zavezanci po tem zakonu, ne glede na to, ali spadajo na področje uporabe tega zakona, lahko prostovoljno priglasijo pomembne incidente, kibernetske grožnje in skorajšnje incidente skupini CSIRT SI-CERT in ji predložijo ustrezne informacije.
Tretji podstavek predloga ureja, da prostovoljna priglasitev skupine CSIRT obravnavajo v skladu s postopkom iz 26. člena tega zakona. Pri prostovoljnem poročanju za priglasitveni subjekt ne veljajo nikakršne dodatne obveznosti, kar pa ne vpliva na preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.
Četrti odstavek predloga nalaga pristojni skupini CSIRT, da po potrebi informacije o priglasitvah, prejetih v skladu s tem členom, kadar je potrebno, posredujejo PNO v vlogi enotne kontaktne točke, pri čemer poskrbijo za zaupnost in ustrezno varstvo informacij, ki jih je posredoval priglasitveni subjekt.
Peti odstavek predloga določa način obdelave prostovoljnih priglasitev. Pristojni skupini CSIRT pred prostovoljnimi priglasitvami lahko prednostno obravnavata obvezne priglasitve. Šesti odstavek predloga določa, da se prostovoljne priglasitve, ki nimajo vpliva ali imajo zanemarljiv vpliv na izvajanje storitev

zavezanih subjektov in imajo zanemarljiv čezmejni vpliv, se obdela le, kadar takšna obdelava skupinama CSIRT ne pomeni nesorazmernega ali neupravičenega bremena.
Sedmi odstavek predloga določa, da se prostovoljna priglasitev ustreznih informacij iz tega člena lahko izvaja tudi po namenski digitalni platformi iz desetega odstavka 26. člena tega zakona.

VI. Vrednotenje incidenta, ocena ogroženosti in ukrepanje

Poglavje vsebuje nacionalne določbe vrednotenja incidentov in ukrepanje ter ocene ogroženosti. Gre za področje, ki je že uveljavljeno v obstoječem Zakonu o informacijski varnosti in razdelano v Nacionalnem načrtu odzivanja na kibernetske incidente. S predlaganimi določbami se kvalitetno nadgrajujejo omenjeni postopki

K 32. členu

Prvi odstavek predloga določa, da priglašene incidente ob njihovem reševanju vrednoti pristojna skupina CSIRT. V primeru, da ima organ državne uprave zagotovljene zmogljivosti vsaj na ravni varnostno operativnega centra, pristojna skupina CSIRT opravi vrednotenje po posvetu z varnostno operativnim centrom. Varnostne dogodke in incidente se vrednoti v naslednje stopnje s poimenovanjem C6 varnostni dogodek, C5 skorajšnji incident, C4 lažji incident, C3 težji incident, C2 težji incident in C1 kritični incident.
Drugi odstavek predloga nalaga PNO, da na podlagi podatkov in stopnje incidenta, ki mu jih sproti posredujejo skupine CSIRT, oceni ali gre hkrati tudi za kibernetski incident velikih razsežnosti ali krizo.
Tretji odstavek predloga nalaga PNO, da mora o kritičnem incidentu nemudoma obvestiti vlado in SNAV, lahko pa ju glede na presojo relevantnih okoliščin obvesti tudi o težjem incidentu kadar obstaja možnost, da preraste v kritični incident.
Četrti odstavek predloga PNO omogoča, da v primeru težjega incidenta C3, C2 ali kritičnega incidenta C1 s pisno odločbo, v nujnih primerih pa tudi ustno, določi takšne primerne in sorazmerne ukrepe, kot je potrebno za zaustavitev incidenta, ki že poteka, ali za odpravo njegovih posledic.
Peti odstavek predloga vzpostavlja postopek, da PNO v primeru, ko nima vseh dejstev nujno potrebnih za opredelitev težjega incidenta ali kritičnega incidenta ter preprečitev nadaljnjih škodljivih posledic incidenta, lahko s pisno odločbo, v nujnih primerih pa tudi ustno od zavezanca, zahteva posredovanje dodatnih podatkov in pojasnil ter določi rok za njihovo posredovanje.
Šesti odstavek predloga nalaga, da PNO določi obseg in časovni okvir za izvedbo ukrepov.
Zoper odločbo iz četrtega in prejšnjega odstavka tega člena ni dovoljena pritožba, dovoljen pa je upravni spor. Tožba v upravnem sporu se vloži na sedežu upravnega sodišča Republike Slovenije. Postopek je nujen in prednosten.
Sedmi odstavek predloga določa, da lahko direktor PNO lahko z namenom preprečitve nastanka krize ali njenega obvladovanja ali zaradi hitrejšega obvladovanja razmer in omejevanja nadaljnjih škodljivih posledic težjega incidenta C2 ali kritičnega incidenta C1 izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih.
Osmi odstavek predloga pa določa, da PNO o ukrepih iz četrtega in sedmega odstavka tega člena obvesti vlado in SNAV.

K 33. členu

Prvi odstavek predloga določa postopek izdelave oceno ogroženosti kibernetske varnosti v Republiki Sloveniji. PNO na podlagi podatkov in informacij, ki se nanašajo na varnost omrežij in informacijskih sistemov, s katerimi razpolaga ali jih pridobi, izdela oceno ogroženost, pri čemer ogroženost vrednoti kot zelo nizka, nizka, srednja, visoka ali kritična. Pri izdelavi ocene ogroženosti se upoštevajo situacijske slike stanja kibernetske varnosti v Republiki Sloveniji, EU in mednarodnem okolju; pridobljena opozorila z mednarodnim sodelovanjem; analize kibernetskih incidentov pri zavezanih subjektih; podatki, ki jih posredujejo deležniki kibernetske varnosti; zaznane ranljivosti omrežij in informacijskih sistemov in podatki pridobljeni s tehničnimi sredstvi za spremljanje stanja in prometa omrežij in informacijskih sistemov.
Drugi odstavek predloga določa, da zavezanci ne glede na oceno ogroženosti izvajajo najmanj ukrepe iz 20. člena tega zakona.

Tretji odstavek predloga določa postopek, ko je ocena ogroženosti ovrednotena kot srednja. PNO o razglasitvi obvesti zavezance in jim pri tem lahko priporoči izvedbo dodatnih ukrepov za varnost omrežij ali informacijskih sistemov. Pristojni nacionalni organ lahko o tem obvesti tudi splošno javnost prek svojih spletnih strani in sredstev javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe.
Četrti odstavek predloga določa postopek, ko je ocena ogroženosti ovrednotena kot kritična. PNO o tem nemudoma obvesti vlado in SNAV, lahko pa ju, glede na presojo relevantnih okoliščin in informacij, obvesti tudi v primeru, da je ogroženost ovrednotena kot visoka. O oceni ogroženosti visoka ali kritična, pristojni nacionalni organ obvesti zavezance, lahko pa obvesti tudi splošno javnost prek svojih spletnih strani in sredstev javnega obveščanja ter lahko hkrati priporoči tudi ustrezne ukrepe. Pristojni nacionalni organ o preklicu ali spremembi ocene ogroženosti kritično, lahko pa tudi visoko obvesti predhodno obveščene deležnike iz tega odstavka.
Peti odstavek predloga določa seznam dodatnih ukrepov, ki jih morajo zavezanci nemudoma pričeti izvajati, ko je ocena ogroženosti visoka.
Šesti odstavek predloga določa seznam dodatnih ukrepov, ki jih morajo zavezanci nemudoma pričeti izvajati, ko je ocena ogroženosti kritična.
Sedmi odstavek predloga omogoča PNO, da zavezancu s pisno odločbo, v nujnih primerih pa tudi ustno, določi primerne in sorazmerne ukrepe, kot je potrebno za zmanjšanje ogroženosti.
Osmi odstavek predloga omejuje PNO, da se ukrepi izdani na podlagi prejšnjega odstavka določijo v takšnem obsegu in za toliko časa, kot je nujno potrebno za dosego namena iz prejšnjega odstavka.
Deveti odstavek predloga omogoča, da direktor PNO lahko z namenom nižanja ocene ogroženosti visoka ali kritična ter posledično zaradi preprečitve nastanka krize ali njenega obvladovanja izda odredbo, s katero odredi izvedbo nujnih ukrepov pri zavezancih, varnostno operativnih centrih oziroma skupinah CSIRT.
Deseti odstavek predloga pa določa, da PNO o ukrepih iz sedmega in devetega odstavka tega člena obvesti vlado in SNAV.

VIII. Kibernetska obramba

Poglavje vsebuje nacionalne določbe kibernetske obrambe na državni ravni, sodelovanje na področju kibernetske obrambe, pomoč na področju kibernetske obrambe ter pomoč pri kibernetski obrambi znotraj Evropske unije in na mednarodni ravni.

Gre za področje, ki je že uveljavljeno v obstoječem Zakonu o informacijski varnosti.

K 34. členu

Prvi odstavek predloga določa plasti kibernetske obrambe, drugi odstavek predloga pa namen kibernetske obrambe.

K 35. členu

S predlogom člena se postavlja sistemski okvir za kibernetsko obrambo in določa ukrepe in dejavnosti kibernetske obrambe na ravni državnih organov. Prvi odstavek predlaganega člena tako določa organe, ki izvajajo usklajene organizacijske, logično-tehnične, tehnične in administrativne ukrepe ter dejavnosti za zagotavljanje celovite kibernetske varnosti skladno s svojimi pristojnostmi. V ta namen PNO vzpostavi koordinacijsko skupino.
Drugi odstavek predloga določa, da organi, ki izvajajo kibernetsko obrambo zagotavljajo ustrezne zmogljivosti za kibernetsko obrambo na področjih, za katere so pristojni. V ta namen lahko vzpostavijo svoje varnostno operativne centre, ki morajo izpolnjevati vsaj minimalni obseg zahtev.
Tretji odstavek predloga določa, da organi stalno spremljajo stanje in odzive na dogodke v kibernetskem prostoru na področju njihovega delovanja.
Četrti odstavek predloga določa postopek vzpostavitve varnostno operativnega centra.
Peti odstavek predloga določa, da se organi za namen izvajanja kibernetske obrambe povezujejo v mednarodne povezave in z aktivnim sodelovanjem v teh povezavah ter prek drugih oblik multilateralnega in bilateralnega sodelovanja.
Šesti odstavek predloga določa obveznost tedenskega in letnega poročanja varnostno operativnih centrov PNO.
Sedmi odstavek predloga določa , da PNO osebam iz tretjega člena Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11, 8/20 in 18/23 – ZDU-1O) omogoči seznanitev z osnovami kibernetske varnosti s kibernetsko higieno.

K 36. členu

Prvi odstavek predloga določa sodelovanje na področju kibernetske obrambe, ki vključuje sklenitev sporazumov o sodelovanju, v katere se po potrebi vključi državne organe, organe lokalne samouprave, gospodarske družbe, zavode in druge organizacije.
Drugi odstavek predloga omogoča, da PNO lahko za namen izvajanja kibernetske obrambe k sodelovanju povabi tudi državljane in državljanke (v nadaljnjem besedilu prostovoljci).
Tretji odstavek predloga določa postopek izbora prostovoljcev in vodenje seznamov.
Četrti odstavek predloga določa pogodbeno razmerja med PNO in prostovoljcem.
Peti odstavek predloga omogoča oblikovanje operativnih skupin za kibernetsko obrambo. Šesti odstavek pa daje pristojnost direktorju PNO, da imenuje vodjo in namestnika posamezne operativne skupine in določa, da administrativno-tehnične pogoje za delovanje operativnih skupin iz prejšnjega (to je petega) odstavka zagotovi pristojni nacionalni organ.

K 37. členu

Predlagani člen omogoča PNO, da lahko nudi zavezancem dodatno pomoč na področju kibernetske obrambe v primeru kibernetskih groženj in incidentov, o katerih pristojni nacionalni organ obvešča vlado in SNAV v skladu s tem zakonom, kot tudi v primeru kibernetskih incidentov velikih razsežnosti ali kriz. Nudenje dodatne pomoči v vsakem posamičnem primeru odobri direktor PNO, pri čemer upošteva vidike nujnosti obvladovanja stanja ali prej opisanih dogodkov, razpoložljivosti operativnih skupin in drugih zmogljivosti za izvajanje kibernetske obrambe ter aktualno oceno kibernetske varnosti v državi.

K 38. členu

Republika Slovenija lahko zaprosi za pomoč pri izvajanju kibernetske obrambe druge države članice Evropske unije oziroma ustrezne institucije, organe, urade in agencij Evropske unije. Republika Slovenija lahko prej navedenim subjektom tudi nudi pomoč pri izvajanju kibernetske obrambe. O prejemu zaprosila pristojnih institucij ali organov druge države ali držav članic Evropske unije za nudenje pomoči pri kibernetski obrambi, pristojni nacionalni organ obvesti SNAV, ki o predlogu odziva na takšno zaprosilo oblikuje stališče in ga posreduje v odločanje vladi.

K 39. členu

Republika Slovenija lahko zaprosi za pomoč pri izvajanju kibernetske obrambe tudi tretje države ali mednarodne organizacije, s katerimi ima sklenjene mednarodne sporazume. Republika Slovenija lahko prej navedenim subjektom tudi nudi pomoč pri izvajanju kibernetske obrambe. Za nudenje in prejem pomoči se smiselno uporabljajo določbe 38. člena. Republika Slovenija lahko sodeluje v skupnih enotah za kibernetsko obrambo, ki jih vzpostavijo mednarodne organizacije, katerih članica je. Odločitev o takšnem sodelovanju, na predlog SNAV, sprejme vlada.

IX. Nadzor

V tem poglavju predlog zakona ureja področje nadzora, in sicer pristojnosti za nadzor, postopek, pravna sredstva ter upravne ukrepe inšpekcijskega organa. Zaradi različne narave zavezancev (bistveni in pomembni) je, upoštevaje člene Direktive 2022/2555 za vsakega od njih predvidena specifičen postopek in dovoljen obseg nadzora.

K 40. členu

V tem predlogu člena gre za prenos določb 31. člena Direktive 2022/2555, ki določa splošne vidike povezane z nadzorom in izvrševanjem.
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 PNO (v nadaljnjem besedilu: inšpektor).
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 predloga določa nalogo, da inšpektor nadzira ali zavezanci izpolnjujejo svoje obveznosti iz tega zakona predvsem z neposrednim vpogledom v podatke, dokumentacijo ter v omrežne in informacijske sisteme; preverjanjem pogojev in načina izvajanja ukrepov za obvladovanje tveganj kibernetske varnosti; pregledom območij, objektov in prostorov zavezancev, kjer se nahajajo ključni, krmilni in nadzorni informacijski sistemi in podatki, pregledom dokumentacije o izvrševanju predpisanih obveznosti obveščanja o kibernetskih incidentih ter drugih obveznostih na podlagi zahtev pristojnih organov iz tega zakona; pregledom poročil o izvedbi revizije informacijskih sistemov in varnostnih pregledov omrežja ter informacijskih sistemov in pregledom druge dokumentacije, potrebne za izvedbo nadzora.
Četrti odstavek predloga določa pristojnosti inšpektorja med tem ko peti odstavek določa obveznosti zavezanca.
Šesti odstavke predloga določa možnost sprožitve upravnega spora zoper odločbo, ki jo izda inšpektor.
Sedmi odstavek predloga ureja podaljšanje rokov v inšpekcijskem postopku. Osmi odstavek predloga daje inšpektorju možnost, da prednostno razvršča izvedbe nadzorov zavezancev.
Deveti odstavek predloga določa, da inšpektor lahko poleg ukrepov, ki jih ima po zakonu, ki ureja inšpekcijski nadzor, odredi tudi ukrepe, določene s tem zakonom, ki jih v skladu z desetim odstavkom podrobneje opredeli.

K 41. členu

V tem predlogu člena gre za prenos določb prvega, drugega, tretjega, devetega in desetega odstavka 32. člena Direktive 2022/2555, ki določa nadzor in izvršilne ukrepe v zvezi z bistvenimi subjekti.
Prvi odstavek predloga določa, da ukrepi, ki jih inšpektor naloži bistvenim subjektom v zvezi z obveznostmi iz tega zakona morajo biti učinkoviti, sorazmerni in odvračilni, pri čemer se upoštevajo okoliščine posameznega primera.
Drugi odstavek predloga opredeljuje pooblastila, ki jih ima inšpektor je pri izvajanju svojih nadzornih nalog pri bistvenih subjektih
Tretji in četrti odstavek predloga določa način izvedbe ciljno usmerjene revizije varnosti ter stroške le-te.
Peti odstavek predloga nalaga inšpektorju, da navede namen zahteve in opredeli zahtevane informacije.
Šesti odstavek predloga določa sodelovanje inšpektorja s pristojno inšpekcijo za področje kritične infrastrukture, kadar izvaja nadzor nad subjektom, ki je na podlagi zakona identificiran kot kritičen.
Sedmi odstavek predloga nalaga inšpektorju, da sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554.

Osmi odstavek predloga določa postopek upravne izvršbe izvršljivih odločb, ki jih je izdal inšpektor v postopku nadzora bistvenih subjektov.
Deveti odstavek predloga določa, da se ukrep iz osmega odstavka ne uporabljajo za pravne osebe javnega prava. Za njihove odgovorne osebe pa se za prisilne ukrepe z izrekanjem denarnih kazni uporabljajo določbe zakona o splošnem upravnem postopku.

K 42. členu

V tem predlogu člena gre za prenos določb od četrtega do desetega odstavka 32. člena Direktive 2022/2555, ki določa nadzor in izvršilne ukrepe v zvezi z bistvenimi subjekti.
Prvi odstavek predloga določa pooblastila, ki jih ima inšpektor pri izvajanju nadzora v zvezi z bistvenimi subjekti.
Drugi odstavek predloga določa ukrepe za odpravo pomanjkljivosti ali izpolnitev zahtev inšpektorja, ko ugotovi, da izrečeni ukrepi niso bili učinkoviti.
Tretji odstavek predloga mogoča začasni preklic ali prepoved, dokler zadevni bistveni subjekt ne sprejme potrebnih ukrepov za odpravo pomanjkljivosti ali ne izpolni zahtev inšpektorja, zaradi katerih je bil tak ukrep uporabljen.
Četrti odstavek predloga določa izjemo, da se ukrepi iz drugega odstavka tega člena ne uporabljajo za subjekte javne uprave, za katere velja ta zakon.
Peti odstavek predloga določa odgovornost odgovorna oseba bistvenega subjekta in odgovarjajo za kršitve svojih dolžnosti v skladu s tem zakonom.
Šesti odstavek predloga določa, da inšpektor pri sprejemanju ukrepov iz tega člena spoštuje postopkovne pravice bistvenega subjekta v postopku nadzora in upošteva okoliščine vsakega posameznega primera.

K 43. členu

V tem predlogu člena gre za prenos določb prvega, drugega, tretjega in šestega odstavka 33. člena Direktive 2022/2555, ki določa nadzor in izvršilne ukrepe v zvezi s pomembnimi subjekti.
Prvi odstavek predloga določa, da se inšpekcijski nadzor pomembnega subjekta se izvede, če inšpektor prejme dokaze, indice ali informacije, da pomembni subjekt ne izvaja ukrepov za obvladovanje tveganj kibernetske varnosti v skladu s predpisanimi obveznostmi iz tega zakona oziroma, da ne izpolnjuje obveznosti v zvezi s obveščanjem o kibernetskih incidentih na predpisan način in v predpisanih rokih ali da ne ravna po zahtevah pristojnega nacionalnega organa iz tega zakona.
Drugi odstavek predloga opredeljuje pooblastila, ki jih ima inšpektor je pri izvajanju svojih nadzornih nalog pri pomembnih subjektih
Tretji in četrti odstavek predloga določata način izvedbe ciljno usmerjene revizije varnosti ter stroške le-te.
Peti odstavek predloga nalaga inšpektorju, da navede namen zahteve in opredeli zahtevane informacije.
Šesti odstavek predloga določa, inšpektor sodeluje z inšpekcijo, ki je pristojna za izvajanje nadzor po uredbi o Uredbe (EU) 2022/2554.
Sedmi odstavek predloga določa postopek upravne izvršbe izvršljivih odločb, ki jih je izdal inšpektor v postopku nadzora bistvenih subjektov.
Osmi odstavek predloga določa, da se ukrep iz osmega odstavka ne uporabljajo za pravne osebe javnega prava. Za njihove odgovorne osebe pa se za prisilne ukrepe z izrekanjem denarnih kazni uporabljajo določbe zakona o splošnem upravnem postopku.

K 44. členu

V tem predlogu člena gre za prenos določb četrtega in petega odstavka 33. člena Direktive 2022/2555, ki določa nadzor in izvršilne ukrepe v zvezi s pomembnimi subjekti.

Prvi odstavek predloga določa pooblastila, ki jih ima inšpektor pri izvajanju nadzora v zvezi s pomembnimi subjekti.
Drugi odstavek predloga določa, da inšpektor pri sprejemanju ukrepov iz tega člena spoštuje postopkovne pravice pomembnega subjekta v postopku nadzora in upošteva okoliščine vsakega posameznega primera.
Tretji odstavek predloga določa odgovornost predstojnik organa subjekta javne uprave ali odgovorna oseba pravne osebe, ki je pomemben subjekt ali deluje kot njen zastopnik na podlagi pooblastila za njegovo zastopanje oziroma odločanje v njegovem imenu je odgovorna oseba za zagotavljanje skladnosti delovanja pomembnega subjekta po tem zakonu (v nadaljnjem besedilu odgovorna oseba pomembnega subjekta) in odgovarjajo za kršitve svojih dolžnosti v skladu s tem zakonom.

K 45 členu

Prvi odstavek predloga določa, da odgovorne osebe zagotovijo, da bistveni subjekti izvajajo oceno skladnosti sprejetih ukrepov za obvladovanje tveganj kibernetske varnosti iz tega zakona in da pomembni subjekti izvajajo oceno skladnosti takšnih ukrepov.
Drugi odstavek določa časovni okvir izvajanja ocene skladnosti bistvenih subjektov med tem ko morajo pomembni subjekti po tretjem odsavku izvesti oceno skladnosti na zahtevo inšpektorja ali v primeru pojava pomembnega incidenta.
Četrti odstavek določa, da poročilo o izvedeni oceni skladnosti pripravi revizor.
Peti in šesti odstavek predloga opredeljujeta dostop inšpektorja do poročila.
Stroške izvedbe ocene skladnosti določa sedmi odstavek predloga.

K 46. členu

V skladu s prvim odstavkom predloga pomembni subjekti opravijo samoocene skladnosti enkrat na dve leti. Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomemben subjekt izpolnjuje zahteve, predpisane s tem zakonom, pomembni subjekti sestavijo izjavo o skladnosti, ki vsebuje potrebne elemente samoocenjevanja skladnosti. Pomembni subjekti so dolžni izjavo iz prejšnjega odstavka tega člena brez odlašanja predložiti inšpektorju, v osmih dneh od njene sestave. Stroške izvajanja samoocene skladnosti nosijo pomembni subjekti.

K 47. členu

Predlog člena določa postopek določitve preizkušenega revizorja za izvedbo revizije varnosti, ki jo zahteva inšpektor po tem zakonu.

K 48. členu

V tem predlogu člena gre za prenos določb 35. člena Direktive 2022/2555, ki opredeljuje kršitve, ki pomenijo kršitev varstva osebnih podatkov.
Prvi odstavek predloga določa da inšpektor o obravnavi zadev iz prvega odstavka 40. člena tega zakona, katerih posledica je kršitev varstva osebnih podatkov, obvešča Informacijskega pooblaščenca brez nepotrebnega odlašanja.
Drugi odstavek predloga opredeljuje postopek, kadar Informacijski pooblaščenec zaradi kršitve določbe točka (i) drugega odstavka 58. člena Uredbe (EU) 2016/679 naloži globo na podlagi zakona, ki ureja varstvo osebnih podatkov.
Tretji odstavek predloga pa določa postopke kadar ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679, sedež v drugi državi članici.

K 49. členu

V tem predlogu člena gre za prenos določb 37. člena Direktive 2022/2555, ki opredeljuje medsebojna pomoč.
Prvi odstavek predloga opredeljuje področje, kadar bistveni ali pomembni subjekt spada v pristojnost pristojnega nacionalnega organa v skladu s 27. členom tega zakona, vendar opravlja storitve v več kot eni državi članici Evropske unije ali opravlja storitve v eni ali več državah članicah Evropske unije, njegovi omrežni in informacijski sistemi pa se nahajajo v drugi državi članici Evropske unije oziroma v več kot eni državi članici Evropske unije, inšpektor lahko izvaja inšpekcijski nadzor nad temi subjekti v sodelovanju s pristojnimi organi nadzora zadevnih drugih držav članic Evropske unije. Inšpektor in pristojni organi nadzora drugih držav članic Evropske unije si medsebojno pomagajo pri izvajanju takega nadzora.
Drugi in tretji odstavek predloga opredeljujeta postopek izvajanja medsebojne pomoči iz prejšnjega odstavka, ki ga izvaja inšpektor preko enotne kontaktne točke ter vsebino zahteve za medsebojno pomoč.
Četrti odstavek predloga opredeljuje postopke inšpektorja, ki jih mora izvesti ob prejemu zahtevka za medsebojno pomoč oziroma ob zavrnitvi le-tega. Po predlaganem petem odstavku se pred zavrnitvijo zahteve za medsebojno pomoč e inšpektor posvetuje z drugimi pristojnim organi nadzora držav članic Evropske unije, ki so tudi pristojne za obravnavo nadzora v konkretnem primeru. Šesti odstavek predloga pa opredeljuje možnost skupnih inšpekcijskih nadzorov.

K 50. členu

V tem predlogu člena gre za način prenosa določb 34. člena Direktive 2022/2555, ki sicer določa splošne pogoje za naložitev upravnih glob bistvenim in pomembnim subjektom, pri čemer se cilj tega čelna navedene direktive zagotavlja preko prekrškovnih sankcij.
Prvi odstavek predloga poleg splošnih pravil za odmero sankcije iz zakona, ki ureja prekrške, pri odločanju o višini izrečene globe za kršitve določb 20., 21., 25. ali 26. člena predlaganega a zakona s strani bistvenih subjektov in pomembnih subjektov upošteva tudi letni promet oziroma letna bilančna vsota bistvenega ali pomembnega subjekta v predhodnem poslovnem letu.
Drugi odstavek predloga določa mejne vrednosti za bistvene subjekte.
Tretji odstavek predloga določa mejne vrednosti za pomembne subjekte.
Četrti odstavek določa, da se pri določanju o naložitvi in višini višine globe iz tega člena upoštevajo okoliščine posameznega primera in vsaj elementi določeni v pravem odstavku 42. člena predlaganega zakona.

K 51. členu

Po predlogu člena se sme za prekrške iz predlaganega zakona v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom.

K 52. členu

Po predlogu člena se do sprememb določb o višinah in razponih glob, ki jih določa zakon, ki ureja prekrške, višine in razponi glob, določeni v 50. členu predlaganega a zakona, uporabljajo ne glede na določbe zakona, ki ureja prekrške.

X. Kazenske določbe

V tem poglavju predloga zakona so predpisane kazni za kršitev njegovih določb. Poglavje obsega prekrške bistvenih subjektov, prekrške pomembnih subjektov in prekrške upravljavca centralnega informacijsko-komunikacijskega sistema.

K 53. členu

Predlog člena določa globe, ki se lahko izrečejo bistvenim subjektom.

K 54. členu

Predlog člena določa globe, ki se lahko izrečejo pomembnim subjektom.

K 55. členu

Predlog člena določa globe, ki se lahko izrečejo upravljavcu centralnega informacijsko-komunikacijskega sistema.

XI. Prehodne določbe

Predlagano poglavje vsebuje določbe glede vzpostavitve samoregistracije, seznamov in obveščanja, prehodnega obdobja za sprejem ukrepov za obvladovanje tveganj in uskladitve obstoječe podatkovne zbirke o registraciji domenskih imen, izdaje podzakonskih predpisov in strategije, prenehanja veljavnosti in podaljšanja uporabe predpisov, sprememb in dopolnitev zakona, ki ureja elektronske komunikacije, dopolnitve zakona, ki ureja prekrške, spremembe zakona, ki ureja varstvo osebnih podatkov ter dokončanja postopkov, začetih pred uporabo tega zakona.

K 56. členu

V predlaganem členu se urejajo roki za vzpostavitev mehanizma za samoregistracijo zavezancev, za vzpostavitev seznama zavezancev in za obveščanje Evropske komisije s strani PNO. Postavljen je tudi rok za seznanitev PNO z identiteto subjektov, ki so na podlagi po učinku enakovrednih obveznosti druge sektorske zakonodaje glede ukrepov in poročanja o incidentih izvzeti iz zadevnih obveznosti po predlaganem zakonu, pri premer so za takšno seznanitev zadolženi pristojni organi druge sektorske zakonodaje
Določa se tudi rok do katerega PNO obvesti Evropsko komisijo o določitvi enotne kontaktne točke, o določitvi organa za obvladovanje kibernetskih kriz, o identiteti skupin CSIRT.
PNO vzpostavi digitalno platformo za medsebojno izmenjava informacij o relevantnih incidentih, kibernetskih grožnjah in skorajšnjih incidentih v enem letu od uveljavitve tega zakona.
Skupine CSIRT in PNO vzpostavijo namensko digitalno platformo iz desetega odstavka 26. člena v enem letu od uveljavitve tega zakona.
Subjekti iz prvega odstavka 28. člena tega zakona o informacijah iz navedene določbe prvič obvestijo pristojni nacionalni organ do 17. januarja 2025, ki te informacije brez nepotrebnega odlašanja prvič posreduje ENISA na način iz četrtega odstavka 28. člena tega zakona.
Registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen vzpostavijo politike in postopke iz tretjega in petega odstavka 29. člena v šestih mesecih od uveljavitve tega zakona.
Organi iz prvega odstavka 35. člena tega zakona pristojni nacionalni organ obvestijo o obstoječih varnostno operativnih centrih, ki izpolnjujejo zahteve iz drugega odstavka 35. člena v tridesetih dneh od uveljavitve tega zakona.

Organi iz prvega odstavka 35. člena tega zakona pristojni nacionalni organ obvestijo o obstoječih varnostno operativnih centrih, ki ne izpolnjujejo zahtev iz drugega odstavka 35. člena v tridesetih dneh od uveljavitve tega zakona, zagotovijo izpolnjevanje le-teh v enem letu od uveljavitve zakona.
Pristojni nacionalni organ v teh mesecih od sprejetja nacionalnega načrt odzivanja iz četrtega odstavka 58. člena tega zakona predloži Evropski komisiji in mreži EU-CyCLONe ustrezne informacije.

K 57. členu

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

K 58. členu

Predlaga se, da v roku osemnajstih mesecev od uveljavitve tega zakona registri TLD imen in subjekti, ki opravljajo storitve registracije domenskih imen uskladijo obstoječe podatkovne zbirke o registraciji domenskih imen z drugim in četrtim odstavkom 29. člena tega zakona za registracije, ki so bile izvedene do uveljavitve tega zakona.

K 59. členu

Predlog člena določa roke za izdajo obveznih podzakonskih predpisov po tem zakonu in za sprejetje Strategije kibernetske varnost 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 60. členu

Predlog člen določa prenehanje veljavnosti predpisov ter smiselno uporabo le-teh do izdaje podzakonskih predpisov sprejetih na podlagi tega zakona.

K 61. členu

S predlogom člena se spremenijo in dopolnijo določbe Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2).
Pojasnjujemo razloge za predlagani poseg v ZEKom-2. Namreč, sedaj veljavni ZInfV v tretjem odstavku 2. člena določa: »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).« S to določbo ZInfV se je takrat sledilo določbi tretjega odstavka 1. člena Direktive 2016/1148/ES ter njeni Uvodni izjavi št. 7. Medtem, ko so bile takšne posebne določbe Uredbe (EU) št. 910/2014 neposredno uporabljive, pa je takratni 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) v slovenski pravni red prenašal takšne posebne zahteve za operaterje iz določb členov 13a in 13b takratne Direktive 2002/21/ES[11]. Medtem je sicer zadnja omenjena direktiva, skupaj s pretežno večino takratnih direktiv s področja elektronskih komunikacij, prenehala veljati v skladu z novo Direktivo

[11] Direktiva evropskega parlamenta in sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva) (UL L 108, z dne 24. 4. 2002, str. 33) (v nadaljnjem besedilu: Direktiva 2002/21/ES

(EU) 2018/1972[12], ki pa je ponovno vsebovala takšne posebne obveznosti za operaterje elektronskih komunikacij in sicer njenih v členih 40 in 41. Direktiva (EU) 2018/1972 je bila prenesena v slovenski pravni red z novim Zakonom elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2), ki v poglavju VIII. Varnost omrežij in storitev ter delovanje v stanjih ogroženosti ureja prenos določb 40. in 41. člena Direktiva (EU) 2018/1972, vsebuje pa tudi nacionalne sektorsko specifične določbe. Nekatere postopkovne in nadzorne določbe so bile dodane tudi zaradi približevanja ureditve z ZInfV in sicer z določitvijo nekaterih nalog v ZEKom-2 tudi za pristojni nacionalni organ iz ZInfV in njegovih inšpektorjev.
Direktiva 2022/2555, ki jo v slovenski pravni red prenašamo s predlaganim zakonom, v členu 42 v Uredbi (EU) št. 910/2024, ki je neposredno uporabljiva, črta 19 člen z učinkom od 18. 10. 2024. V členu 43 pa ista direktiva posega v Direktivo (EU) 2018/1972 in v njej črta člena 40 in 41, prav tako z učinkom od 18. oktobra 2024. Pri tem je treba še dodati, da za razliko od ZInfV in direktive, ki se je z njim prenesla v slovenski pravni red, predlagani ZInfV-1 obe prej navedeni področji urejanja oziroma subjektov, ki v tem sektorju delujejo, ne izključuje več iz področja uporabe predlaganega zakona, kar je razvidno iz 3. člena (področje uporabe) in pripadajočih prilog tega zakona, ki povzemata Prilogi I in II Direktive 2022/2555 razvidno tudi iz Priloge I tega zakona (Visoko kritični sektorji) tako ponudniki storitev zaupanja, kot tudi ponudniki javnih komunikacijskih omrežij in ponudniki javno dostopnih elektronskih komunikacijskih storitev spadajo med vrste subjektov, ki sodijo v (visoko kritični) sektor »8. Digitalna infrastruktura« omenjene Priloge I. Prav tako so te kategorije sedaj izrecno navedene med zavezanci iz 6. člena predlaganega zakona.
Iz zgoraj opisanih razlogov je treba s predlaganim zakonom poseči v ZEKom-2, ki je Direktivo (EU) 2018/1972 prenesel v slovenski pravni red in sicer iz razloga, da ne bi prišlo do neskladnosti z EU pravnim redom ter da se prepreči podvajanje urejanja zadevnih obveznosti zavezancev, ki bodo po novem urejene z ZInfV. Ob tem dodajamo, da so predlagani posegi v ZEKom-2 predvsem tisti, ki so nujni za medsebojno usklajenost obeh zakonov. Sektorsko specifične dodatne rešitve oziroma ukrepi v ZEKom-2 glede varnosti in celovitosti omrežij in storitev, ki jih predlagani zakon ne ureja (kot tudi ne ureja takšnih rešitev oziroma ukrepov za ostale sektorje), torej ostajajo v ZEKom-2 oziroma so bili, kjer smo to ocenili za potrebno, le minimalno spremenjeni oziroma dopolnjeni z vidika jasnosti in ob upoštevanju razvoja stanja varnostnih tveganj v praksi.
Po predlaganem členu zato z dnem uveljavitve predlaganega zakona prenehajo veljati določbe 115., 118., 119., 120., 121., 122. in 123. člena poglavja VIII. Varnost omrežij in storitev ter delovanje v stanjih ogroženosti iz ZEKom- 2, prav tako prenehata veljati tudi splošna akta izdana na podlagi sedmega odstavka 115. in iz drugega odstavka 118. člena ZEKom-2, ki se smiselno uporabljata do izdaje podzakonskih predpisov sprejetih na podlagi tega zakona.
S predlaganim členom se spreminjajo oziroma dopolnijo tudi določbe prvega, drugega, četrtega in petega odstavka 116. člena, četrtega odstavka 124. člena, 128. člena VIII. poglavja ZEKom-2. Posledično se v poglavju XV. Nadzor spreminjajo tudi določbe prvega odstavka 287.člena in 288. člen ter črta tretji odstavek 289. člena ZEKom-2. V poglavju XVII. Kazenske določbe ZEKom-2 pa v členu 299. (prekrški) črtajo točke 22, 23, 24, 26, 27, 28, 29 in 30.

K 62. členu

Predlog člena ureja poseg v Zakonu o prekrških (Uradni list RS, št. 29/11 – uradno prečiščeno besedilo, 21/13, 111/13, 74/14 – odl. US, 92/14 – odl. US, 32/16, 15/17 – odl. US, 73/19 – odl. US, 175/20 – ZIUOPDVE in 5/21 – odl. US), v katerega se ustrezno umešča informacijska varnost.

K 63. členu

[12] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (UL L št. 321 z dne 17. 12. 2018, str. 36) (v nadaljnjem besedilu: Direktiva 2018/1972/EU).

Predlog člena zaradi uskladitve s tema zakonom posega v Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22).

K 64. členu

Upravni, inšpekcijski in prekrškovni postopki, ki do začetka uporabe tega zakona še niso bili pravnomočno končani, se po predlogu tega člena končajo v skladu z dosedanjimi predpisi.

XII. Končna določba

K 65. členu

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