|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Številka: 007-66/2023-36 | | | | | | |
| Ljubljana, 15. 5. 2024 | | | | | | |
| EVA 2023-1544-0005 | | | | | | |
| GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE  [gp.gs@gov.si](mailto:gp.gs@gov.si) | | | | | | |
| **ZADEVA:** **Zakon o informacijski varnosti (EVA 2023-1544-0005) – predlog za obravnavo, redni postopek** | | | | | | | | | | | |
| **1. Predlog sklepov vlade:** | | | | | | | | | | | |
| Na podlagi drugega odstavka 2. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17 in 163/22) je Vlada Republike Slovenije na ........... seji dne .......... pod točko ....... sprejela sklep:  Vlada Republike Slovenije je določila besedilo predloga Zakona o informacijski varnosti (EVA 2023-1544-0005) in ga pošlje v obravnavo Državnemu zboru Republike Slovenije po rednem postopku.    Barbara Kolenko Helbl  GENERALNA SEKRETARKA  Prejmejo:   * Vsa ministrstva in vladne službe, * Skupnosti občin Slovenije, * Združenju občin Slovenije, * Združenju mestnih občin Slovenije.   Priloge:   * besedilo predloga zakona, | | | | | | | | | | | |
| **2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:** | | | | | | | | | | | |
| / | | | | | | | | | | | |
| **3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:** | | | | | | | | | | | |
| * dr. Uroš Svete, direktor Urada Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu URSIV), * Kory Golob, pomočnik direktorja URSIV, * Mag. Melita Šinkovec, vodja Sektorja za informacijsko in kibernetsko varnost, URSIV, * Barbara Pernuš Grošelj, sekretarka, Sektor za informacijsko in kibernetsko varnost, URSIV. | | | | | | | | | | | |
| **3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:** | | | | | | | | | | | |
| Pri pripravi dela ali celotnega gradiva niso sodelovali zunanji strokovnjaki. | | | | | | | | | | | |
| **4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:** | | | | | | | | | | | |
| * dr. Uroš Svete, direktor Urada Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu URSIV), * Kory Golob, pomočnik direktorja URSIV, * Mag. Melita Šinkovec, vodja Sektorja za informacijsko in kibernetsko varnost, URSIV, * Barbara Pernuš Grošelj, sekretarka, Sektor za informacijsko in kibernetsko varnost, URSIV. | | | | | | | | | | | |
| **5. Kratek povzetek gradiva:** | | | | | | | | | | | |
| Predloga novega Zakona o informacijski varnosti (ZInfV-1) bo nadomestil Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23). Poglavitni namen priprave novega zakona je prenos sekundarne zakonodaje Evropske unije v pravni red Republike Slovenije. S predlaganim novim ZInfV-1 v svoj pravni red prenašamo Direktivo (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) št. 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 (EU) 2022/2555). Namen predlaganega zakona je sistemska ureditev področja informacijske oziroma kibernetske varnosti in zagotovitev visoke ravni kibernetske varnosti vključno s krepitvijo zaupanja v proizvode IKT, storitve IKT in postopke IKT ter njihove 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. Predlagani zakon tako vsebuje določbe, ki prenašajo Direktivo (EU) 2022/2555 kot tudi nacionalne določbe za doseganje namena zakona v Republiki Sloveniji. Z zakonom se ureja tudi izvajanje Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L št. 151 z dne 7. 6. 2019, str. 15; v nadaljnjem besedilu: Uredba (EU) 2019/881).  Od začetka veljavnosti ZInfV je bil dosežen velik napredek pri zviševanju ravni kibernetske odpornosti v Republiki Slovenije. Vzpostavljen je bil institucionalni okvir in regulatorni okvir za kibernetsko varnost v državi. Z implementacijo Direktive (EU) 2016/1148 smo vzpostavili nacionalni okvir za varnost omrežij in informacijskih sistemov. Nacionalne zmogljivosti smo povezali z bistveno infrastrukturo in subjekti, ki jih je določila Vlada Republike Slovenije. V Slovenije smo poleg izvajalcev bistvenih storitev in ponudnikov digitalnih storitev identificirali tudi organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti ter povezane subjekte, ki se povezujejo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom. Zaradi pomena kritične infrastrukture smo določili, da so izvajalci bistvenih storitev tudi tisti upravljavci kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo področje kritične infrastrukture, in nosilce obrambnega načrtovanja, ki so določeni v skladu s predpisi, ki urejajo področje obrambe, katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov.  Kljub tem dosežkom pa so bile pri pregledu Direktive (EU) 2016/1148 razkrite pomanjkljivosti, zaradi katerih z navedeno direktivo ni mogoče učinkovito obravnavati sedanjih in nastajajočih izzivov na področju kibernetske varnosti.  Poglavitni poudarki, ki jih prinaša Direktiva (EU) 2022/2555 so, da direktiva določa obveznosti za ponudnike digitalnih storitev, vključno s ponudniki stičišča omrežij, ponudniki storitev DNS, razen upravljavcev korenskih imenskih strežnikov, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebin, ponudniki storitev zaupanja, ponudniki javnih elektronskih komunikacijskih omrežij in ponudniki javno dostopnih elektronskih komunikacijskih storitev. Direktiva razširja obseg sektorjev, ki so vključeni v okvir varnosti omrežij in informacijskih sistemov, na kritično infrastrukturo, ki je ključnega pomena za delovanje družbe in gospodarstva. Določa obveznost oblikovanja nacionalne strategije za varnost omrežij in informacijskih sistemov ter vzpostaviti sodelovanje med organi pregona, regulatorji, informacijskimi varnostnimi agencijami in drugimi ustreznimi organi. Uvaja strožje zahteve za poročanje o varnostnih incidentih s strani ponudnikov digitalne infrastrukture in drugih zavezancev ter določa kriterije za ocenjevanje resnosti incidentov. Spodbuja izmenjavo informacij in sodelovanje med državami članicami EU, zlasti v zvezi z varnostnimi incidenti, ki lahko vplivajo na več držav.  Poleg prenosa določb Direktiva (EU) 2022/2555 z osnutkom predloga ZInfV-1 izboljšujemo zakonsko ureditev v delu, ko gre za nacionalne določbe. Predlog zakona v največji meri ohranja strukturo Direktiva (EU) 2022/2555 in jo nadgrajuje s poglavjema VII. Vrednotenje incidenta, ocena ogroženosti in ukrepanje in VIII. Kibernetska obramba. Z ohranitvijo, razširitvijo in nadgraditvijo vsebin iz obstoječega zakona v novem ZInfV-1 sledimo ugotovitvam iz vaj kriznega odzivanja in koordinacije med deležniki kibernetske varnosti. Ti postopki odzivanja so zasnovani z namenom izboljšanja odpornosti in varnosti omrežij in informacijskih sistemov pred kibernetskimi grožnjami ter zagotavljanja učinkovitejšega odziva na morebitne incidente. | | | | | | | | | | | |
| **6. Presoja posledic za:** | | | | | | | | | | | |
| a) | javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih | | | | | | | | | **DA** | |
| b) | usklajenost slovenskega pravnega reda s pravnim redom Evropske unije | | | | | | | | | **DA** | |
| c) | administrativne posledice | | | | | | | | | **DA** | |
| č) | gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij | | | | | | | | | **DA** | |
| d) | okolje, vključno s prostorskimi in varstvenimi vidiki | | | | | | | | | **DA** | |
| e) | socialno področje | | | | | | | | | **NE** | |
| f) | dokumente razvojnega načrtovanja:   * nacionalne dokumente razvojnega načrtovanja * razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna * razvojne dokumente Evropske unije in mednarodnih organizacij | | | | | | | | | **NE** | |
| **7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:**  Predlog zakona ima finančne posledice. | | | | | | | | | | | |
| **I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu** | | | | | | | | | | | |
|  | | | Tekoče leto (t) | | t + 1 | t + 2 | | | | | t + 3 |
| Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna | | |  | |  |  | | | | |  |
| Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov | | |  | |  |  | | | | |  |
| Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna | | |  | |  |  | | | | |  |
| Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov | | |  | |  |  | | | | |  |
| Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva | | |  | |  |  | | | | |  |
| **II. Finančne posledice za državni proračun** | | | | | | | | | | | |
| **II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:** | | | | | | | | | | | |
| Ime proračunskega uporabnika | | Šifra in naziv ukrepa, projekta | | Šifra in naziv proračunske postavke | | Znesek za tekoče leto (t) | | | | | Znesek za t + 1 |
|  | |  | |  | |  | | | | |  |
|  | |  | |  | |  | | | | |  |
| **SKUPAJ** | | | | | |  | | | | |  |
| **II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:** | | | | | | | | | | | |
| Ime proračunskega uporabnika | | Šifra in naziv ukrepa, projekta | | Šifra in naziv proračunske postavke | | Znesek za tekoče leto (t) | | | | | Znesek za t + 1 |
|  | |  | |  | |  | | | | |  |
|  | |  | |  | |  | | | | |  |
| **SKUPAJ** | | | | | |  | | | | |  |
| **II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:** | | | | | | | | | | | |
| Novi prihodki | | | | Znesek za tekoče leto (t) | | | | Znesek za t + 1 | | | |
|  | | | |  | | | |  | | | |
|  | | | |  | | | |  | | | |
|  | | | |  | | | |  | | | |
| **SKUPAJ** | | | |  | | | |  | | | |
| **OBRAZLOŽITEV:**   1. **Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu**   V zvezi s predlaganim vladnim gradivom se navedejo predvidene spremembe (povečanje, zmanjšanje):   * prihodkov državnega proračuna in občinskih proračunov, * odhodkov državnega proračuna, ki niso načrtovani na ukrepih oziroma projektih sprejetih proračunov, * obveznosti za druga javnofinančna sredstva (drugi viri), ki niso načrtovana na ukrepih oziroma projektih sprejetih proračunov.  1. **Finančne posledice za državni proračun**   Prikazane morajo biti finančne posledice za državni proračun, ki so na proračunskih postavkah načrtovane v dinamiki projektov oziroma ukrepov:  **II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:**  Navedejo se proračunski uporabnik, ki financira projekt oziroma ukrep; projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in proračunske postavke (kot proračunski vir financiranja), na katerih so v celoti ali delno zagotovljene pravice porabe (v tem primeru je nujna povezava s točko II.b). Pri uvrstitvi novega projekta oziroma ukrepa v načrt razvojnih programov se navedejo:   * proračunski uporabnik, ki bo financiral novi projekt oziroma ukrep, * projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in * proračunske postavke.   Za zagotovitev pravic porabe na proračunskih postavkah, s katerih se bo financiral novi projekt oziroma ukrep, je treba izpolniti tudi točko II.b, saj je za novi projekt oziroma ukrep mogoče zagotoviti pravice porabe le s prerazporeditvijo s proračunskih postavk, s katerih se financirajo že sprejeti oziroma veljavni projekti in ukrepi.  **II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:**  Navedejo se proračunski uporabniki, sprejeti (veljavni) ukrepi oziroma projekti, ki jih proračunski uporabnik izvaja, in proračunske postavke tega proračunskega uporabnika, ki so v dinamiki teh projektov oziroma ukrepov ter s katerih se bodo s prerazporeditvijo zagotovile pravice porabe za dodatne aktivnosti pri obstoječih projektih oziroma ukrepih ali novih projektih oziroma ukrepih, navedenih v točki II.a.  **II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:**  Če se povečani odhodki (pravice porabe) ne bodo zagotovili tako, kot je določeno v točkah II.a in II.b, je povečanje odhodkov in izdatkov proračuna mogoče na podlagi zakona, ki ureja izvrševanje državnega proračuna (npr. priliv namenskih sredstev EU). Ukrepanje ob zmanjšanju prihodkov in prejemkov proračuna je določeno z zakonom, ki ureja javne finance, in zakonom, ki ureja izvrševanje državnega proračuna. | | | | | | | | | | | |
| **7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:** | | | | | | | | | | | |
| **8. Predstavitev sodelovanja z združenji občin:** | | | | | | | | | | | |
| Vsebina predloženega gradiva (predpisa) vpliva na:   * pristojnosti občin, * delovanje občin, * financiranje občin. | | | | | | | | | **DA** | | |
| Gradivo (predpis) je bilo poslano v mnenje:   * Skupnosti občin Slovenije SOS: **NE (bo poslano)** * Združenju občin Slovenije ZOS:  **NE (bo poslano)** * Združenju mestnih občin Slovenije ZMOS:  **NE (bo poslano)**   Predlogi in pripombe združenj so bili upoštevani:   * v celoti, * večinoma, * delno, * niso bili upoštevani.   Bistveni predlogi in pripombe, ki niso bili upoštevani.  / | | | | | | | | | | | |
| **9. Predstavitev sodelovanja javnosti:** | | | | | | | | | | | |
| Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja: | | | | | | | | | **DA** | | |
| Javna obravnava na e-demokracija 16. 2. 2024 – 18. 3. 2024  <https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16290>  Izvedena bo ponovna javna obravnava hkrati z medresorskim usklajevanjem. | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:** | | | | | | | | | **NE (bo upoštevano)** | | |
| **11. Gradivo je uvrščeno v delovni program vlade:** | | | | | | | | | **DA** | | |
| Dr. Uroš Svete  direktor urada  Priloge:   * besedilo predloga zakona | | | | | | | | | | | |

**PRILOGA 3 (jedro gradiva)**

**PREDLOG**

**(EVA 2023-1544-0005)**

**PREDLOG**

**ZAKONA O INFORMACIJSKI VARNOSTI**

**I. UVOD**

**1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA**

Leta 2016 je Vlada Republike Slovenije sprejela Strategijo kibernetske varnosti, ki je podlaga za pripravo in izvedbo ukrepov na področju zagotavljanja informacijske varnosti. Strategija kibernetske varnosti poudarja pomen vzpostavitve celovitega sistema zagotavljanja kibernetske varnosti kot pomembnega dejavnika varnosti države, ki bo prispeval k zagotovitvi odprtega, varnega in varovanega kibernetskega prostora ter bo podlaga za nemoteno delovanje infrastrukture, pomembne za delovanje državnih organov, gospodarstva in za življenje vsakega posameznika.

17. aprila 2018 je Državni zbor Republike Slovenij sprejel Zakon o informacijski varnosti (v nadaljevanju besedila: ZInfV), ki ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji. Določa minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona. Prav tako ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost, enotne kontaktne točke za informacijsko varnost, nacionalne skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij in skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave na področju zagotavljanja informacijske varnosti. Zakon je določil tri kategorije zavezancev: izvajalce bistvenih storitev, organe državne uprave in ponudnike digitalnih storitev. Uredil je tudi področje nadzora, ki je v pristojnosti inšpekcijskega organa, ki je notranja organizacijska enota pristojnega nacionalnega organa za informacijsko varnost. Zakon ne velja za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve ter ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 (tako imenovana Uredba eIDAS).

Republika Slovenija do sprejema ZInfV ni imela zakonsko urejenega področja zagotavljanja informacijske varnosti. S sprejemom ZInfV smo v slovenski pravni red prenesli Direktivo 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: Direktiva 2016/1148/ES) ter se primerno odzvali na naraščajoče trend obsega in kompleksnosti incidentov v kibernetskem prostoru. Zaradi velike odvisnost gospodarstva ter celotne družbe od neprekinjenega delovanja omrežij in informacijskih sistemov nujna celovita ureditev in tudi okrepitev področja zagotavljanja informacijske varnosti. Državo k temu spodbujajo in jo hkrati zavezujejo tudi sprejeti strateški domači in mednarodni dokumenti, na primer Resolucija o strategiji nacionalne varnosti Republike Slovenije (Uradni list RS, št. 59/19). Omenjena resolucija je informacijsko-kibernetske grožnje opredelila kot eno ključnih groženj. Svet za nacionalno varnost (SNAV) je na seji 4. maja 2020 sklenil, da Slovenija potrebuje skupno in celovito delovanje na področju kibernetske varnosti. V okviru predsedovanja Svetu EU v drugi polovici leta 2021 je bila za eno od strateških tem določena digitalizacija, znotraj nje pa kot prednostno vprašanje ravno kibernetska varnost. Evropska komisija in Evropska služba za zunanje delovanje sta decembra 2020 predstavili novo strategijo EU za kibernetsko varnost. Njen namen je narediti Evropo odpornejšo proti kibernetskim grožnjam ter zagotoviti, da bodo lahko vsi državljani in podjetja uživali vse koristi, ki jih nudijo zaupanja vredne in zanesljive storitve ter digitalna orodja. Svet EU je 22. marca 2021 sprejel sklepe o strategiji za kibernetsko varnost, v katerih je poudaril, da je kibernetska varnost bistvena za izgradnjo odporne, zelene in digitalne Evrope.

Na podlagi strateških usmeritev in zaznanih pomanjkljivosti sistema informacijsko/kibernetske varnosti je bil ZInfV nadgrajen z ustreznimi spremembami in dopolnitvami. Novela Zakona o spremembah in dopolnitvi Zakona o informacijski varnosti (v nadaljnjem besedilu: ZInfV-A), ki jo je Državni zbor Republike Slovenije sprejel 4. junija 2021, je pristojni nacionalni organ za informacijsko varnost, ki je deloval kot organ v sestavi Ministrstva za javno upravo, preoblikovala v samostojno vladno službo. S tem se je sledilo nacionalnim in mednarodnim izkušnjam, da so pristojni nacionalni organi za področje informacijske (kibernetske) varnosti postali ključni deležniki v sistemu zagotavljanja nacionalne varnosti sodobnih držav. Z ustrezno umestitvijo pristojnega nacionalnega organa, ki je prevzel tudi naloge pripravljanja predlogov predpisov s področja informacijske in kibernetske varnosti ter izvajanje nalog nacionalnega certifikacijskega organa za kibernetsko varnost, smo okrepili proaktivno vlogo na področju informacijsko kibernetske varnosti. Novela zakona je tudi določila, da naloge CSIRT organov državne uprave izvaja notranja organizacijska enota pristojnega nacionalnega organa.

S spremembo Zakona o vladi (ZVRS-J) in posledičnimi spremembami in dopolnitvami Zakona o državni upravi (ZDU-1O) je pristojnost upravljanja s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom (v nadaljnjem besedilu: centralni informacijsko-komunikacijski sistem) iz ministrstva, pristojnega za javno upravo, ki je (bilo) pristojno za informacijsko varnost v centralnem informacijsko-komunikacijskim sistemom, prešla na novo ministrstvo, za digitalno preobrazbo. Izvajanja enotne informacijske varnostne politike se je preneslo na pristojni nacionalni organ za informacijsko varnost. Novela zakona je tudi nadgradila pristojnosti in naloge CSIRT organov državne uprave ter obveznosti upravitelja centralnega informacijsko-komunikacijskega sistema. Novela je uvedla tudi ustrezne nadzorstvene določbe za nove subjekte.

**Organiziranost nacionalnega sistema kibernetske varnosti**

Nacionalni sistem informacijske/kibernetske varnosti je razdeljen na tri ravni:

- strateško-koordinacijsko (URSIV kot pristojni nacionalni organ za informacijsko varnost – PNO);

- operativno oziroma raven zaznavanja in odzivanja na incidente (SI-CERT kot nacionalni CSIRT, SIGOV-CERT kot CSIRT organov državne uprave in varnostno-operativni centri MNZ/Policija, SOVA, MO, MDP);

- raven zavezancev (izvajalci bistvenih storitev, ponudniki digitalnih storitev, organi državne uprave, povezani subjekti).

Osrednja naloga PNO na strateški koordinacijski ravni nacionalnega sistema informacijske/kibernetske varnosti je skrb za pripravo in izvajanje strategije ter normativno urejanje področja kibernetske varnosti. Naloga PNO je usklajevanje organov in organizacij, ki delujejo na področju informacijske/kibernetske varnosti (nacionalni CSIRT, CSIRT organov državne uprave, varnostno-operativni centri, regulatorji oziroma nadzorniki področij iz drugega odstavka 5. člena ZInfV, Agencija za komunikacijska omrežja in storitve Republike Slovenije, Informacijski pooblaščenec, organi kazenskega pregona in ponudniki varnostnih rešitev), ter v odnosu do mednarodnih deležnikov. Za zagotavljanje čezmejnega sodelovanja URSIV izvaja naloge enotne kontaktne točke, kar pomeni predvsem sooblikovanje politik na tem vsebinskem področju v okviru organizacij EU, NATO, OVSE, OZN. V zvezi s tem sta ključna izmenjava in usklajevanje stališč z drugimi pristojnimi organi na državni ravni (MO, MNZ, MZZ, SOVA, UVTP, SI-CERT). S tega vidika se izvaja tudi redno letno poročanje glede na vprašalnike NATA in EU (ENISA).

Na operativni ravni sistema so zmogljivosti za odzivanje na incidente v kibernetskem prostoru porazdeljene med SI-CERT kot nacionalni odzivni center za omrežne incidente, SIGOV-CERT kot CSIRT organov državne uprave, ki deluje v okviru PNO ter varnostno operativne centre Ministrstva za obrambo, Slovenske obveščevalno-varnostne agencije, Policije in Ministrstva za digitalno preobrazbo.

**Direktiva (EU) 2022/2555**

Namen 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) št. 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 (EU) 2022/2555) je določiti ukrepe, katerih cilj je zagotoviti visoko skupno raven kibernetske varnosti v Evropski uniji, da bi se izboljšalo delovanje notranjega trga. V ta namen direktiva določa obveznosti, ki od držav članic zahtevajo, da sprejmejo:

- nacionalne strategije za kibernetsko varnost in imenujejo ali ustanovijo pristojne organe, organe za obvladovanje kibernetskih kriz, enotne kontaktne točke za kibernetsko varnost (v nadaljnjem besedilu: enotne kontaktne točke) in skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT);

- ukrepe za obvladovanja tveganj za kibernetsko varnost in obveznosti poročanja za subjekte vrste iz Priloge I ali II, kot tudi za subjekte, ki so identificirani kot kritični subjekti na podlagi Direktive (EU) 2022/2557;

- pravila in obveznosti glede izmenjave informacij o kibernetski varnosti;

- obveznosti nadzora in izvrševanja za države članice.

Direktiva (EU) 2022/2555 prinaša veliko sprememb na področju kibernetske varnosti in vpliva ne le na subjekte, ki so že zavezanci po ZInfV in morajo varovati svoje informacijske sisteme v skladu z veljavnim ZInfV, ampak tudi na veliko število subjektov, ki jih bo nova ureditev zajela in doslej niso bili dolžni izpolnjevati nobenih obveznosti ter so incidente priglašali na prostovoljni podlagi. Direktiva krepi skupno situacijsko zavedanje in kolektivno sposobnost odzivanja na kibernetske napade znotraj Evropske unije. V ta namen razširja področje uporabe ter odpravlja razlikovanje med izvajalci bistvenih storitev in ponudniki digitalnih storitev z uvedbo splošnega merila velikosti (vključitev srednjih in velikih podjetij). Direktiva prav tako krepi varnostne zahteve za podjetja z uvedbo delovanja za obvladovanje tveganj kot osnovne zahteve zagotavljanja kibernetske varnosti, vključno s prenosom odgovornosti na vodstva podjetij. S tem se naj bi močno izboljšala odpornost in zmogljivost odzivanja, naj si gre za javne ali zasebne subjekte kot tudi Evropske unije kot celote, na incidente na področju kibernetske varnosti in zaščite kritične infrastrukture.

Določa tudi strožje nadzorne ukrepe, uvaja medsebojne strokovne preglede držav članic Evropske unije, okrepljeno varnost dobavnih verig ter vzpostavljamo osnovni okvir za usklajeno razkritje ranljivosti.

Direktiva (EU) 2022/2555 pomeni minimalno stopnjo harmonizacije, ki državam članicam ne preprečuje, da na nacionalnih ravneh sprejmejo še dodatne ukrepe za dvig odpornosti na kibernetske incidente.

Obseg Direktiva (EU) 2022/2555 je bistveno razširjen v primerjavi z Direktive (EU) 2016/1148 in ni več nujno povezan s predhodno identifikacijo s strani pristojnih nacionalnih organov. Zavezanec je zajet, če deluje v enem od sektorjev in opravlja storitev, ki je navedena v Prilogi 1 in 2 in se uvršča po velikosti. Direktiva (EU) 2022/2555 dodaja nove sektorje. Dodaja tudi vrste subjektov znotraj obstoječih sektorjev. Sektorji so razdeljeni v dve skupini.

Visoko kritični sektorji (Priloga 1) so:

* Energetika (elektrika, daljinsko ogrevanje in hlajenje, nafta, zemeljski plin, vodik)
* Promet (zrak, železnica, voda, cestni)
* Bančništvo
* Infrastruktura finančnih trgov
* Zdravje (ki ne vključuje več samo bolnišnic, ampak tudi referenčne laboratorije, proizvajalce medicinskih pripomočkov ali farmacevtskih pripravkov in druge)
* Pitna voda
* Odpadne vode
* Digitalna infrastruktura
* Upravljanje s storitvami IKT
* Javna uprava (centralna in regionalna)
* Vesolje

Drugi kritični sektorji (Priloga 2) so:

* Poštne in kurirske storitve
* Ravnanje z odpadki
* Izdelava, proizvodnja in distribucija kemikalij
* Pridelava, predelava in distribucija živil
* Proizvodnja (proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov; proizvodnja računalnikov, elektronskih in optičnih izdelkov; proizvodnja električnih naprav; proizvodnja drugih strojev in naprav; proizvodnja motornih vozil, prikolic in polprikolic; proizvodnja drugih vozil in plovil)
* Digitalni ponudniki
* Raziskave

Razen izjem, v NIS 2 ni več aktivne identifikacije. Podjetje, ki deluje v zgoraj navedenih sektorjih, je zavezanec, če je veliko ali srednje podjetje. To pomeni, da mora imeti subjekt več kot 50 zaposlenih in letni promet ali letno bilančno vsoto več kot 10 milijonov evrov. Z določenimi izjemami so iz obsega direktive izključena mala in mikro podjetja (z manj kot 50 zaposlenimi in letnim prometom (ali letnim skupnim bilančnim izkazom) manj kot 10 milijonov evrov - kumulativni pogoji).

Prejšnja razlika med izvajalci bistvenih storitev in ponudniki digitalnih storitev je nadomeščena z razlikovanjem med bistvenimi in pomembnimi subjekti. Razlika med bistvenimi in pomembnimi subjekti je predvsem v nadzoru in sankcijah.

Bistveni subjekti so velika podjetja, ki spadajo v sektorje visoke kritičnosti, navedene v Prilogi 1 direktive. Veliko podjetje je opredeljeno kot podjetje z vsaj 250 zaposlenimi in z letnim prometom vsaj 50 milijonov evrov ali letnim skupnim bilančnim izkazom vsaj 43 milijonov evrov.

Pomembni subjekti so srednje velika podjetja, ki delujejo v sektorjih visoke kritičnosti iz Priloge 1 direktive in velika ali srednje velika podjetja v sektorjih iz Priloge 2 direktive, ki ne spadajo v kategorijo bistvenega subjekta (zaradi njihove velikosti ali vrste subjekta). Srednje veliko podjetje je opredeljeno kot podjetje z vsaj 50 zaposlenimi ali z letnim prometom (ali skupnim bilančnim izkazom) vsaj 10 milijonov evrov, vendar z manj kot 250 zaposlenimi in ne več kot 50 milijoni evrov letnega prometa ali 43 milijoni evrov skupnega letnega bilančnega izkaza.

Ob tem obstajajo nekatere izjeme. V nekaterih sektorjih so subjekti, ne glede na velikost, določeni kot bistveni. Taki primeri so ponudniki javnih elektronskih komunikacijskih omrežij, subjekti, določeni kot kritični na nacionalni ravni v skladu s predpisom, ki ureja kritično infrastrukturo, subjekti javnega sektorja (na centralni ravni), kvalificirani ponudniki storitev zaupanja in registri imen domen najvišje ravni ter ponudniki storitev DNS.

Poleg tega lahko država članica posebej določi subjekte kot bistvene ali pomembne, če gre za edinega ponudnika storitev ali ko bi motnja v zagotavljanju storitev lahko imela pomembne posledice za javno red, javno varnost ali javno zdravje.

Direktiva (EU) 2022/2555 uvaja načelo teritorialnost glede na sedež subjekta. Vendar pa obstajajo izjeme od tega pravila teritorialne pristojnosti. Ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javnih elektronskih komunikacijskih storitev so podvrženi pristojnosti države članice, v kateri ponujajo svoje storitve. Ponudniki storitev DNS, registri imen domen najvišje ravni, subjekti, ki ponujajo storitve registracije imen domen, ponudniki storitev oblakov, ponudniki storitev podatkovnih centrov, ponudniki storitev dostave vsebine, upravljani ponudniki storitev, upravljani ponudniki storitev varnosti, pa tudi ponudniki spletnih tržnic, iskalnikov ali platform za družabna omrežja so podvrženi pristojnosti države članice, v kateri imajo svoj glavni sedež v Evropski uniji.

Bistveni in pomembni subjekti morajo sprejeti ustrezne in sorazmerne ukrepe za upravljanje tveganj za varnost svojih omrežij in informacijskih sistemov ter preprečevanje incidentov ali omilitev posledic incidentov za prejemnike svojih storitev in za druge storitve. Ukrepi morajo temeljiti na celovitem pristopu k vsem nevarnostim. Namen je zaščititi omrežja in informacijske sisteme ter fizično okolje teh sistemov pred incidenti. Upravni organi ali izvršni organi bistvenih in pomembnih subjektov morajo odobriti ukrepe za upravljanje tveganj kibernetske varnosti in nadzorovati njihovo izvajanje, lahko pa so tudi odgovorni za kakršne koli kršitve. Na nacionalni ravni lahko pristojni organi natančneje predpišejo izpolnjevanje varnostnih zahtev. Evropska komisija bo sprejela izvedbeni akt, ki bo določil tehnične in metodološke zahteve za ukrepe za upravljanje tveganj kibernetske varnosti.

Pomembni in bistveni subjekti morajo brez odlašanja poročati o vsakem pomembnem incidentu pristojni skupini CSIRT. Pomemben incident je tisti, ki je povzročil ali je sposoben povzročiti resne operativne motnje pri storitvah v sektorjih ali podsektorjih, navedenih v Prilogah 1 in 2 direktive, ali finančne izgube za prizadeti subjekt; ali je vplival ali je sposoben vplivati na druge fizične ali pravne osebe z ustvarjanjem znatne materialne ali nematerialne škode. Direktiva (EU) 2022/2555 določa postopke obveščanja ter zavezuje subjekt tudi k obveščanju prejemnikov njihov storitev. Pomembni in bistveni subjekti lahko prostovoljno priglasijo ostale incidente, kibernetske grožnje in preprečene incidente. Prostovoljna priglasitev je omogočena tudi subjektom, ki ne spadajo med bistvene in pomembne.

Države članice morajo zagotoviti, da subjekti iz Direktive (EU) 2022/2555 sprejmejo potrebne ukrepe in poročajo o incidentih. Za to lahko na primer izvajajo redne zunanje revizije ali preglede ali zahtevajo določeno dokumentacijo. Pristojni nacionalni organi bi morali imeti tudi pooblastila za ukrepanje, da bi spodbudili subjekte k sprejetju ustreznih ukrepov. To se lahko giblje od izdaje opozoril ali zavezujočih navodil za odpravo pomanjkljivosti do obveščanja njihovih strank. Poleg teh upravnih ukrepov se lahko uvedejo tudi učinkovite, sorazmerne in odvračilne upravne globe. Kršitve ukrepov za upravljanje tveganj ali poročil o incidentih se lahko kaznujejo. Za bistvene subjekte: z upravnimi globami v višini do 10.000.000 evrov ali vsaj 2 % skupnega letnega svetovnega prometa v preteklem davčnem letu podjetja, ki spada v bistveni subjekt, ne glede na to, kateri znesek je višji. Za pomembne subjekte: upravne globe v višini do 7.000.000 evrov ali vsaj 1,4 % skupnega letnega svetovnega prometa v preteklem davčnem letu podjetja, ki spada v pomemben subjekt, ne glede na to, kateri znesek je višji.

**2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA**

**2.1 Cilji**

Republika Slovenija bo z Zakonom o informacijski varnosti (v nadaljnjem besedilu:: ZInfV-1) v svoj pravni red prenesla Direktivo (EU) 2022/2555, katere namen 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.

Ker je Direktiva (EU) 2022/2555 uvedla pomembne spremembe v obstoječi regulativni okvir je bila sprejeta odločitev, da se pripravi nov zakon, ki ureja področje informacijske varnosti, ki bo nadomestil obstoječi zakon, a ohranil in nadgradil pozitivne rešitve. Nov predlog zakona za temelj smiselno ohranja besedilo obstoječega zakona ter izpolnjuje minimalne zahteve določene v Direktivi (EU) 2022/2555. V tekstu se odražajo večletne izkušnje koordinacije kibernetske varnosti v Republiki Sloveniji. Osnutek ZInfV-1 združuje obstoječo razdrobljeno upravljanje kibernetske varnosti ob upoštevanju specifičnega področja bančništva in instrumentov finančnih trgov. Zakon ustrezno naslovi razmerje do zakona s področja kritične infrastrukture.

**2.2 Načela**

Predlog zakona, podobno kot Direktive (EU) 2022/2555, upošteva spoštovanje človekovih pravic in temeljnih svoboščin, zlasti pravico do spoštovanja zasebnega življenja in komunikacij, varstvo osebnih podatkov, svobodo gospodarske pobude, lastninsko pravico, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča ter pravico podati izjavo. Ob tem predlog zakona upošteva tudi načelo ekonomičnosti (v smislu preprečevanja podvajanja administrativnih bremen) ter načela pravne države, in sicer pravne varnosti in sorazmernosti.

**2.3 Poglavitne rešitve**

* Predstavitev predlaganih rešitev

V nadaljevanju so po poglavjih predstavljene poglavitne rešitve predloga zakona.

**I. Splošne določbe**

* vsebina predloga zakona ureja področje informacijske 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 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 iz kritičnih sektorjev ter zavezancev, ki so 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 (EU) 2022/2555);
* s tem zakonom se ureja izvajanje Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L št. 151 z dne 7. 6. 2019, str. 15; v nadaljnjem besedilu: Uredba (EU) 2019/881);
* pomen izrazovje skladen z Direktivo (EU) 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;
* zakon uvaja tudi kategorijo varovani podatki pristojnega nacionalnega organ. Organizacijske in logično tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenja zbirk podatkov katerih upravljavec je pristojni nacionalni organ določi predstojnik omenjenega organa.

**II. Zavezanci**

* zavezanci po predlogu zakona se delijo na bistvene in pomembne subjekte;
* zavezanci so javni ali zasebni subjekti vrste iz Prilog Direktive (EU) 2022/2555 I ali II (v nadaljnjem besedilu Priloga I ali II), ki imajo vsaj 50 zaposlenih in letni promet ali letno bilančno vsoto vsaj 10 milijonov evrov;
* zavezanci 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; ter subjekti lokalne samouprave in sicer mestne občine in občine, ki imajo sedeže v krajih, kjer so sedeži upravnih enot;
* pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev;
* zavezanci 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;
* skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRTI)
* predlog zakona določa, zahteve in tehnične zmogljivosti skupin CSIRT, njihove naloge ter sodelovanje skupin CSIRT z deležniki zasebnega sektorja;
* koordinatorja za usklajeno razkrivanje ranljivosti v Republiki Sloveniji (v nadaljnjem besedilu koordinator), ki deluje kot zaupanja vreden posrednik;
* predlog zakona opredeljuje sodelovanje na nacionalni ravni in 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;
* za zagotavljanje visoke ravni informacijske in kibernetske varnosti in odpornosti svojih omrežnih in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki temeljita na pristopu upoštevanja vseh nevarnosti;
* v skladu z določbami tega zakona so določeni ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov;
* 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 pomoč 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 (EU) 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 (EU) 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**

* zakon določa roke za izdajo podzakonskih aktov vzpostavitev samoregistracijskega mehanizma in namenskih platform;
* ureja veljavnost zakon in določa roke, do katerih morajo bistveni in povezani subjekti izpolniti obveznosti iz 20. in 21. člena tega zakona.

**XII. Končna določba**

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

Skladno z zgoraj zapisanim se s predlogom zakona v pravni red prenaša Direktiva (EU) 2022/2555, katere cilj in namen 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. Poleg tega se bo z zakonom sistemsko uredilo in nadgradilo področje kibernetske obrambe tako na strateški kot tudi na operativni ravni nacionalnega sistema zagotavljanja informacijske varnosti.

Na podlagi predloga zakona pristojni nacionalni organ vzpostavi mehanizem za samoregistracijo zavezancev iz 6. člena tega zakona po prvem odstavku 7. člena tega zakona v roku dveh mesecev od uveljavitve; vzpostavi digitalno platformo za medsebojno izmenjava informacij o relevantnih incidentih, kibernetskih grožnjah in skorajšnjih incidentih iz drugega odstavka 17. člena tega zakona ter namensko digitalno platformo iz desetega odstavka 26. člena v enem letu od uveljavitve tega zakona. Poleg tega se zaradi uskladitev z nalogami pristojnega nacionalnega organa, ki je samostojna vladna služba, uskladi Odlok o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za informacijsko varnost (Uradni list RS, št. 114/21 in 69/23) s tem zakonom v treh mesecih od njegove uveljavitve,

Z dnem uveljavitve tega zakona preneha veljati Zakon o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23). Prav tako prenehajo veljati na njegovi osnovi izdani podzakonski akti, ki pa se smiselno uporabljajo do izdaje podzakonskih predpisov sprejetih na podlagi tega zakona.

* **Normativna usklajenost predloga zakona**

Predlog zakona je usklajen z veljavno zakonodajo ter s splošno veljavnimi načeli mednarodnega prava in z mednarodnimi pogodbami, ki obvezujejo RS. Predlog zakona prenaša Direktivo (EU) 2022/2555.

* **Usklajenost predloga zakona**

Delovni osnutek predloga zakona je bil ob koncu leta 2023 posredovana deležnikom zastopanim v Koordinacijski skupini za kibernetsko varnost. Na podlagi pobud so bili opravljeni usklajevalni sestanki in predstavitve osnutkov.

Osnutek predloga zakona je bil od 16. februarja do 18. marca 2024 v javni obravnavi.

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

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

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

Pri pripravi ocene finančnih posledic predloga zakona je bila upoštevana preliminarna ocena o povečanju števila zavezance. Ocena kaže, da bo v Republiki Slovenije registriranih prek 1.000 subjektov. Gre za enajstkratno povečanje števila zavezancev, ki se bo neposredno odrazilo v delovanju pristojnega nacionalnega organa, skupinah CSIRT, varnostno operativnih centrih in nadzornem organu. V luči obvladovanja skupnosti kibernetske varnosti bo potrebno okrepiti koordinacijo deležnikov, dvigniti sodelovanje med organi ter pristopiti k iskanju novih rešitev. Slednje vidimo v vpeljavi mehanizma za samoregistracijo, platformi za priglasitev incidentov in platformi za izmenjavo informacij. Ob tem ne smemo pozabiti na kadrovsko popolnjenost in ustrezen načrte izobraževanja in usposabljanja.

Z vzpostavitvijo in okrepitvijo delovanjem organov za izvajanje nalog skladno s predlogom ZInfV-1 bodo nastale finančne posledice za državni proračun zaradi:

1. zagotovitve pogojev za delovanje pristojnega nacionalnega organa, vključno z zagotovitvijo pogojev za
   * delovanje enotne kontaktne točke za kibernetsko varnost;
   * delovanje organa za obvladovanje kibernetskih kriz;
   * izvajanje nalog organa za obvladovanje incidentov velikih razsežnosti in kriz;
   * izvajanje certifikacijskih shem za kibernetsko varnost;
   * izpolnjevanje zakonskih pogojev za delovanje SIGOV-CERT;
   * okrepljeno delovanje Inšpekcije za informacijsko varnost.
2. zagotovitve zakonskih pogojev za delovanje skupin CSIRT ter pogojev za izvajanje nalog usklajenega razkrivanje ranljivosti.
3. zagotovitev pogojev za delovanje ali vzpostavitev varnostno operativnih centrov organov državne uprave;

Pri oceni potrebnih finančnih sredstev je pri točkah 1 do 3 upoštevan letni bruto 2 znesek plače zaposlenega, skupaj s povračili stroškov in drugimi prejemki iz delovnega razmerja, v višini 45.000 eurov ter enkraten strošek vzpostavitve posameznega delovnega mesta v višini 5.000 eurov in letni strošek kasnejšega delovanja v višini 2.000 eurov na posamezno delovno mesto. V oceni je prav tako upoštevan letni strošek službenih poti in izobraževanja v višini 1.200 EUR na zaposlenega. Ker se bo ZInfV-1 predvidoma pričel izvajati ob koncu leta 2024, so stroški za leto 2024 temu ustrezno prilagojeni (znižani) oziroma je upoštevano obstoječe stanje.

**Skupni ocenjeni stroški za delovanja organov skladno s predlogom ZInfV-1:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **t** | **t + 1** | **t + 2** | **t + 3** |
|  | **Kategorija/leto** | **2024** | **2025** | **2026** | **2027** |
| 1. | Število zaposlitev kumulativno |  |  |  |  |
| 2. | Plače |  |  |  |  |
| 3. | Materialni stroški |  |  |  |  |
| 4. | Investicije in investicijsko vzdrževanje |  |  |  |  |
| 5. | Dvig ravni informacijske varnosti |  |  |  |  |
| 6. | Nakup/pridobitev prostorov |  |  |  |  |
|  | **Skupaj** |  |  |  |  |

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

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

1. **Zagotovitev pogojev za delovanje pristojnega nacionalnega organa:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **t** | **t + 1** | **t + 2** | **t + 3** |
|  | **Kategorija/leto** | **2024** | **2025** | **2026** | **2027** |
|  | **Število zaposlitev kumulativno** | **36** | **45** | **60** | **70** |
| 1 | Plače | 1.563.884 € | 2.025.000 € | 2.700.000 € | 3.150.000 € |
| 2 | Materialni stroški | 958.962 € | 674.000 € | 764.000 € | 822.000 € |
| 3 | Investicije in investicijsko vzdrževanje | 585.096 € | 819.400 € | 1.040.200 € | 1.509.000 € |
| 4 | Dvig ravni informacijske varnosti | 217.456 € | 845.000 € | 958.500 € | 1.049.350 € |
|  | **Skupaj** | 3.325.398 € | **4.363.400 €** | **5.462.700 €** | **6.530.350 €** |

Ocena temelji na projekciji končnega števila novih zaposlitev po letih, in sicer v letu 2024 36, v letu 2025 45, v letu 2026 60 in 2027 70 zaposlitev, in pripadajočih stroških ter stroških za investicije v strojno in programsko opremo, ne vključuje pa stroškov nakupa oziroma pridobitve prostorov. V letu 2024 je za namen opravljanja nalog PNO na URSIV, vključno z administrativno podporo (kadrovsko, finančno, pravno) predvidenih sedem novih zaposlitve. Potrebna finančna sredstva v višini 3.325.398 eurov za leto 2024 za delovanje PNO in pripravo na izvajanje novih naloge iz tega zakona so zagotovljena v proračunu URSIV.

V letu 2025 so za namen opravljanja nalog PNO predvidene še nove zaposlitve, ki bodo realizirane v krepitvi Inšpekcije za informacijsko varnost, Sektorja za informacijsko in kibernetsko varnost ter SIGOV-CERT. Presoja zagotovitve dodatnih zaposlitev bo izvedena v skladu s sprejetjem Zakona o izvrševanju proračuna RS za leti 2025 in 2026 ter sprejetimi sklepi Vlade RS o kadrovskih načrtih organov državne uprave.

V letu 2026 je predvidena nadaljnja kadrovska krepitev, s katerimi bomo prednost okrepili delovanje SIGOV-CERT, področje certifikacije in delovanje enotne kontaktne točka. V letu 2027 bomo zakrožili krepitev nadzornega in odzivnega dela ter certifikacije.

1. **Zagotovitev pogojev za delovanje skupin CSIRT in varnostno operativnih centrov organov državne uprave:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **t** | **t + 1** | **t + 2** | **t + 3** |
|  | **Kategorija/leto** | **2024** | **2025** | **2026** | **2027** |
| 1. | Delovanje skupine CSIRT | 843.998 € | 928.398 € | 1.021.238 € | 1.123.362 € |
| 2. | VOC Policija |  |  |  |  |
| 3. | VOC MDP |  |  |  |  |
| 4. | Kibernetski center OVS |  |  |  |  |
| 5. | VOC SOVA |  |  |  |  |

Ocena temelji na projekciji končnega števila novih zaposlitev po letih, in sicer v letu 2024 xxx, v letu 2025 xxx ter v letih 2026 in 2027 xxx zaposlitve, in pripadajočih stroških ter stroških za investicije v strojno in programsko opremo za obvladovanje incidentov.

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

Za izvajanje zakona so za leto 2024 zagotovljena sredstva v državnem proračunu, in sicer v okviru Urada Vlade Republike Slovenije za informacijsko varnost, Ministrstva za obrambo, Ministrstva za digitalno preobrazbo, Ministrstva za notranje zadeve in Slovenske obveščevalno-varnostne agencije.

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

**Prikaz ureditve v pravnem redu EU**

Predlog zakona je usklajen s pravnim redom EU.

**Prikaz ureditve v najmanj treh pravnih sistemih držav članic EU**

Za primerjanje stanja na področju, ki ureja ukrepe za doseganje o ukrepih za visoko skupno raven kibernetske varnosti v Evropski uniji, v nadaljevanju predstavljamo predvidene zakonodajne rešitve treh držav, in sicer Italijanske republike, Češke republike in Francoske republike.

**Italijanska republika**

Pristojni nacionalni organ za kibernetsko varnost je agencija za kibernetsko varnost (AgID). Zakonodajni odlok z dne 18. maja 2018, št. 65, za izvajanje Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o določitvi ukrepov za visoko skupno raven varnosti omrežja in informacijskih sistemov v Uniji v določbi 19. člena določa inšpekcijska pooblastila za dejavnosti inšpekcij in preverjanj, potrebnih za nadzor nad izvajanjem ukrepov iz 12., 13., 14. in 15. člena tega odloka, italijanskemu pristojnemu nacionalnemu organu, to je agenciji za kibernetsko varnost.

V okviru agencije za kibernetsko varnost deluje tudi skupina za odzivanje na kibernetske grožnje in incidente (CSIRT). CSIRT Italije je odgovoren za usklajevanje in podporo dejavnosti nacionalne mreže CSIRT, ki vključuje skupine CSIRT iz različnih sektorjev, vključno z vlado, kritično infrastrukturo in zasebnimi podjetji. AgID svojim članom zagotavlja tudi tehnično pomoč, upravljanje incidentov in storitve za izmenjavo informacij. Skupina CSIRT tesno sodeluje tudi z drugimi nacionalnimi in mednarodnimi organizacijami, da bi zagotovila pripravljenost Italije na odzivanje na kibernetske grožnje in incidente.

V Italiji izvajanje zakona po direktivi NIS 2 še ni uradno implementirano. Osnutek zakona, ki bo na italijansko vlado prenesel pooblastilo za izdajo zakonodajnega odloka za izvajanje direktive NIS 2, čaka na sprejem s strani parlamenta. Načeloma bodo ohranili ureditev kot so jo imeli do sedaj. Strmijo k okrepljenemu obvladovanju kibernetskih kriz z nacionalno celico za kibernetsko varnost (NCS) in agencijo v njenem jedru. Aktualni nadzorni organ je »Agenzia per la Cybersicurezza Nazionale« (krajše »ACN«) oziroma Nacionalna agencija za kibernetsko varnost (AgID). Trenutno besedilo osnutka zakona o prenosu pooblastil določa, da bo ACN potrjen kot ustrezni organ direktive NIS 2. Med trenutnimi pristojnostmi ACN je regulativna dejavnost, vključno z izvajanjem direktive NIS 2: Autorità e sanzioni – Agenzia per la cybersicurezza nazionale.

Kar se tiče CSIRT-a in tehnične podpore strmijo k popolni integraciji s EU, NATO-m in ostalimi mednarodno relevantnimi mehanizmi. Poleg tega imajo v nacionalni strategiji osem ukrepov, namenjenih nacionalnim kibernetskim storitvam, vključno s HyperSOC, HPC in ISAC (podprt s skladi za okrevanje in odpornost)

**Češka republika**

Pristojni nacionalni organ ima oddelek za zakonsko urejanje, ki skrbi za zadeve, povezane z zakonom št. 181/2014, zb. z dne 23. julija 2014, o kibernetski varnosti in spremembi povezanih zakonov (zakon o kibernetski varnosti), ter službo za revizijo, ki nadzoruje izpolnjevanje zahtev iz zakona o kibernetski varnosti pri zavezancih. Skupaj z oddelkom za zakonsko urejanje sodeluje pri pripravi zakonodaje s področja kibernetske varnosti in zagotavlja metodološko podporo zavezancem. Služba za revizijo sodeluje z drugimi revizijskimi organi, katerih dejavnosti na področju kibernetske varnosti se prekrivajo.

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

**Francoska republika**

Francoska nacionalna agencija za kibernetsko varnost (*Agence nationale de la sécurité des systèmes d’information* – ANSSI) je bila ustanovljena z odlokom št. 2009-834 z dne 7. julija 2009 kot nacionalni organ. Kot pristojni nacionalni organ za kibernetsko obrambo ter varnost omrežij in informacij v skladu z direktivo (NIS) ANSSI nudi strokovno znanje in pomoč državnim organom in izvajalcem bistvenih storitev. Skrbi za promocijo francoskih tehnologij, sistemov in znanja. Ima vlogo pri gradnji zaupanja v digitalnem okolju. V skladu s cilji iz Bele knjige o obrambi in nacionalni varnosti iz leta 2013 ima ANSSI vlogo pri usmerjanju francoskih in evropskih raziskav kibernetske varnosti. ANSSI se po potrebi opira na strokovno znanje strateškega odbora, sestavljenega iz visokih državnih uradnikov.

Zakon št. 2018-133 z dne 26. februarja 2018 o različnih določbah za prilagoditev pravu Evropske unije na področju varnosti v določbi 8. člena določa, da predsednik vlade lahko operaterje, javne ali zasebne, ki ponujajo storitve, ki so bistvenega pomena za delovanje družbe ali gospodarstva in katerih nepretrgano delovanje bi lahko resno ogrozili incidenti, ki vplivajo na omrežja in informacijske sisteme, potrebne za zagotavljanje navedenih storitev, podvrže pregledom, namenjenim preverjanju izpolnjevanja obveznosti iz poglavja v zvezi z varnostjo omrežij in informacijskih sistemov operaterjev bistvenih storitev ter z ravnjo varnosti omrežij in informacijskih sistemov, potrebnih za zagotavljanje bistvenih storitev. Preglede dokumentov in na kraju samem izvaja nacionalni organ za varnost informacijskih sistemov, naveden v členu L. 2321-1 obrambnega zakonika, ali ponudniki storitev, ki jih pooblasti predsednik vlade. Stroške kontrol poravnajo operaterji. Člen L. 2321-2-1 obrambnega zakonika pooblašča ANSSI, da za namene opredelitve groženj uporabi napravo za zaznavanje v omrežju operaterja elektronskih komunikacij ali na informacijah ponudnika dostopa ali gostitelja.

Odlok št. 2018-384 z dne 23. maja 2018 o varnosti omrežij in informacijskih sistemov operaterjev bistvenih storitev in ponudnikov digitalnih storitev v določbi 13. člena določa, da predsednik vlade po posvetovanju z zadevnimi ministri obvesti izvajalce bistvenih storitev o svoji odločitvi o uvedbi nadzora iz 8. člena zakona št. 2018-133 z dne 26. februarja 2018 o različnih določbah za prilagoditev pravu Evropske unije na področju varnosti. Navedeni zakon določa cilje in obseg nadzora ter rok, v katerem se nadzor izvede. V zakonu je tudi navedeno, glede na naravo dejavnosti, ki se izvajajo, ali ta nadzor izvaja nacionalna agencija za varnost informacijskih sistemov ali usposobljeni ponudnik storitev. V drugem primeru operater izbere ponudnika storitve s seznama, ki mu ga pošlje, in o tem takoj obvesti nacionalno agencijo za varnost informacijskih sistemov.

Ocenjujejo, da bo implementacija Direktivo (EU) 2022/2555. vplivala na tisoče subjektov v več kot osemnajstih panogah, ki bodo sedaj regulirane. Kot nacionalni organ na področju digitalne varnosti bo ANSSI še vedno skrbel za izvajanje podpornih programov za organizacije, prilagojenih njihovemu profilu. Izvajal bo vsakodnevno svetovanje, izmenjavo strokovnega znanja in operativne pomoči, hkrati pa spodbujal razvoj varnostnih izdelkov in storitev zaupanja. Ohranili bodo glavni cilj - dvigniti splošno raven digitalne varnosti v Franciji, tako da se zavezanim subjektom omogoči, da se bolje zaščitijo pred grožnjami

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

**6. PRESOJA POSLEDIC, KI JIH BO IMEL SPREJEM ZAKONA**

**6.1 Presoja administrativnih posledic:**

**a) V postopkih oziroma poslovanju javne uprave ali pravosodnih organov:**

Pristojni nacionalni organ ohranja status samostojne vladne službe in nadgrajuje svoje pristojnosti z okrepljenim delovanjem na področju certificiranja kibernetske varnosti, enotne kontaktne točke in organa za obvladovanje kibernetskih kriz. Ohranja se ureditev, da sta notranji organizacijski enoti PNO skupina CSIRT državne uprave in Inšpekcija za informacijsko varnost.

Vlada RS je sprejela Odlok o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za informacijsko varnost (Uradni list RS, št. 114/21 in 69/23) s katerim je opredelila naloge pristojnega nacionalnega organa, ki je URSIV. V okviru nacionalnega sistema informacijske varnosti je URSIV tako pristojni organ na strateški ravni. Na operativni ravni sistema pa so zmogljivosti za odzivanje na incidente v kibernetskem prostoru porazdeljene med SI-CERT kot nacionalni odzivni center za omrežne incidente in SIGOV-CERT - CSIRT organov državne uprave, ki je notranja organizacijska enota pristojnega nacionalnega organa, Ministrstvo za digitalno preobrazbo (MDP) pristojno za upravljanje informacijsko-komunikacijskih sistemov, Ministrstvo za obrambo (MO) za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami, Slovensko obveščevalno-varnostno agencijo (SOVA) na področju protiobveščevalnega delovanja ter Policijo, Urad za informatiko in telekomunikacije in Upravo kriminalistične policije, predvsem Center za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala. Organi na obeh ravneh sistema so podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju.

RS je do zdaj imela zakonsko urejeno področje zagotavljanja informacijske varnosti v Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23). Ob tem je treba pojasniti, da za pravne ali fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve (v nadaljnjem besedilu: operaterji), veljajo posebne obveznosti glede varnosti in celovitosti omrežij in storitev iz VII. poglavja (Varnost omrežij in storitev ter delovanje v izjemnih stanjih) Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17; v nadaljnjem besedilu: ZEKom-1), kjer gre za prenos 13.a in 13.b člena Direktive 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (Okvirna direktiva). Operaterji morajo namreč sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev, zlasti zaradi preprečevanja in zmanjševanja učinkov varnostnih incidentov na uporabnike in medsebojno povezana omrežja. Sprejeti ukrepi morajo ob upoštevanju stanja zagotoviti raven varnosti, primerno predvidenemu tveganju. Določene so tudi obveznosti obveščanja in poročanja o kršitvah varnosti ali celovitosti Agenciji za komunikacijska omrežja in storitve RS (v nadaljnjem besedilu: AKOS), ki potem po potrebi poroča UVTP. Iz tega razloga Direktiva 2016/1148/ES v tretjem odstavku 1. člena operaterje izključuje iz svojega dometa, temu pa sledi tudi predlog ZIV. Določbe ZInfV se ne uporabljajo tudi za ponudnike storitev zaupanja, za katere veljajo zahteve iz 19. člena Uredbe (EU) št. 910/2014 (tako imenovana Uredba eIDAS).

Naraščajoči trend obsega in kompleksnost incidentov v kibernetskem prostoru in velika odvisnost gospodarstva ter celotne družbe od neprekinjenega delovanja omrežij in informacijskih sistemov pa zahtevajo celovito ureditev in tudi okrepitev področja zagotavljanja informacijske varnosti. Državo k temu zavezujejo tudi sprejeti strateški domači in mednarodni dokumenti, na primer Resolucija o strategiji nacionalne varnosti RS, Strategija kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor« ter nacionalna Strategija kibernetske varnosti in predvsem Direktiva (EU 2022/2555, ki se prenaša s predlogom tega zakona.

Glede na zgoraj navedeno potrebnih nalog in pristojnosti ni mogoče celovito in sistemsko izvajati v nobenem od zgoraj navedenih organov, saj je za dosego ciljev na področju informacijske varnosti treba zagotoviti in okrepiti ustrezno koordinacijo med vsemi resorji in organi. Omenjeno nalogo ohranja pristojni nacionalni organ.

Glede skupin CSIRT je treba pojasniti, da zakon gradi na trenutnem stanju z željo po prehodu v bolj kompleksne oblike delovanja, ki so primerno umeščene v nacionalno varnostni sistem Republike Slovenije. Ob tem se z novim zakonom več energije posveča tudi varnostno operativnim centom organov državne uprave.

**b) Pri obveznostih strank do javne uprave ali pravosodnih organov:**

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

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

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

Predlog zakona namreč med področja, na katerih delujejo bistveni in pomembni subjekti (zavezanci po tem zakonu), uvršča tudi sektorja pitna in odpadna voda ter ravnanje z odpadki. S tem ko bodo zavezanci iz omenjenih sektorjev poskrbeli za ustrezno raven varnosti svojih omrežij in informacijskih sistemov skladno s tem zakonom, se bo zmanjšala njihova ranljivost v primeru pomembnih incidentov, ki bi sicer lahko imeli negativne posledice. Prav tako se bodo ob ustrezni priglasitvi incidentov pristojni skupini CSIRT in ob sodelovanju z njim ter pristojnim nacionalnim organom lahko zmanjšali tudi že nastali negativni vplivi incidentov na obe področji.

**6.3 Presoja posledic za gospodarstvo:**

Predlog zakona ima vpliv na gospodarstvo, saj so med zavezanci v večini gospodarski subjekti. Po predlogu zakona so bistveni in pomembni subjekti (zavezancev) namreč lahko javni ali zasebni subjekti, ki spadajo v katerega od v zakonu določenih področij: energetika, promet, bančništvo, infrastruktura finančnih trgov, zdravje, pitna voda, odpadne vode, digitalna infrastruktura, upravljanje s storitvami IKT, vesolje, poštne in kurirske storitve, ravnanje z odpadki, izdelava, proizvodnja in distribucija kemikalij, pridelava, predelava in distribucija živil, proizvodnja (proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov; proizvodnja računalnikov, elektronskih in optičnih izdelkov; proizvodnja električnih naprav; proizvodnja drugih strojev in naprav; proizvodnja motornih vozil, prikolic in polprikolic; proizvodnja drugih vozil in plovil), digitalni ponudniki in raziskav

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

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

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

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

**6.4 Presoja posledic za socialno področje:**

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

**6.5 Presoja posledic za dokumente razvojnega načrtovanja:**

Ukrepi iz predloga zakona bodo pripomogli k uresničevanju ciljev že sprejetih strateških domačih in mednarodnih dokumentov, na primer Resolucije o strategiji nacionalne varnosti Republike Slovenije, Strategije kibernetske varnosti Evropske unije »Odprt, varen in zavarovan kibernetski prostor« in leta 2016 sprejete nacionalne Strategije kibernetske varnosti ter Direktive (EU) 2022/2555.

Zaradi uskladitve z Direktive (EU) 2022/2555. predlog zakona prinaša še nekatere dodatne elemente, ki jih bo treba vključiti v novo Strategijo kibernetske varnosti, zaradi česar se v prehodnih določbah predvideva sprejem strategije (skladno s tem zakonom) v roku enega leta od njegove uveljavitve.

**6.6 Presoja posledic za druga področja:**

Zakon ne bo imel posledic na drugih področjih.

**6.7 Izvajanje sprejetega predpisa:**

1. Predstavitev sprejetega zakona

Sprejeti zakon bo objavljen na spletnih straneh Urada Vlade Republike Slovenije za informacijsko varnost.

1. Spremljanje izvajanja sprejetega predpisa

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

Inšpekcijski nadzor bo izvajal pristojni nacionalni organ oziroma njegova organizacijska enota Inšpekcija za informacijsko varnost.

Vlada bo moralo v enem letu od uveljavitve zakona izdati z zakonom predvidene predpise in strategije.

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

Drugih posebnih pomembnih okoliščin v zvezi z vprašanji, ki jih ureja predlog zakona, ni.

**7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA:**

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

Pri pripravi zakona niso sodelovali zunanji strokovnjaki ali pravne osebe.

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

* dr. Uroš Svete, direktor Urada Republike Slovenije za informacijsko varnost (v nadaljnjem besedilu URSIV),
* Kory Golob, pomočnik direktorja URSIV,
* Mag. Melita Šinkovec, vodja Sektorja za informacijsko in kibernetsko varnost, URSIV,
* Barbara Pernuš Grošelj, sekretarka, Sektor za informacijsko in kibernetsko varnost, URSIV.