REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 83 30
F: 01 478 83 31
E: gp.mju@gov.si
www.mju.gov.si

Številka: 007-443/2021/5
Ljubljana, 12. maj 2021
EVA 2021-3130-0020
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE gp.gs@gov.si

ZADEVA: Zakon o spremembah in dopolnitvi Zakona o informacijski varnosti (EVA 2021-3130-0020) – predlog za obravnavo – NOVO GRADIVO št. 1

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 in 55/17) je Vlada Republike Slovenije na ..... seji dne ..... pod točko ..... sprejela sklep:

Vlada Republike Slovenije je določila besedilo predloga Zakona o spremembah in dopolnitvi Zakona o informacijski varnosti (EVA 2021-3130-0020) in ga pošlje v obravnavo Državnemu zboru Republike Slovenije po nujnem postopku.

mag. Janja Garvas Hočevar
vršilka dolžnosti generalnega sekretarja

Priloga:
- besedilo predloga zakona.

Prejmejo:
- Državni zbor Republike Slovenije,
- Ministrstvo za javno upravo,
- Ministrstvo za finance,
- Ministrstvo za obrambo,
- Ministrstvo za notranje zadeve,
- Služba Vlade Republike Slovenije za zakonodajo.

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

Predlaga se nujni postopek obravnave predloga zakona v Državnem zboru Republike Slovenije na podlagi prvega odstavka 143. člena Poslovnika državnega zbora (Uradni list RS, št. 92/07 – uradno prečiščeno besedilo, 105/10, 80/13,38/17 in 46/20), ker je sprejem zakona nujen zaradi interesov varnosti države in da se preprečijo težko popravljive posledice za delovanje države.

Veljavni Zakon o informacijski varnosti (Uradni list RS, št. 30/18) določa, umestitev pristojnega nacionalnega organa kot organ v sestavi Ministrstva za javno upravo.

Nacionalne in mednarodne izkušnje kažejo, da so pristojni nacionalni organi za področje informacijske (kibernetske) varnosti postali ključni deležniki v sistemu zagotavljanja nacionalne varnosti sodobnih držav. Zavedati se moramo, da je digitalizacija vseprisotna, za njen razvoj se bo namenjalo vedno več sredstev, širila se bo v vse družbene podsisteme, potrebno pa bo zagotavljati visoko stopnjo informacijske varnosti.

Nujno je potrebno vzpostaviti čimprejšnje mednarodne izmenjave podatkov v mreži CSIRT in okrepiti mednarodno sodelovanje med nacionalnimi organi. Pri obravnavi zadnjih incidentov in koordinaciji aktivnosti le-teh so bile zaznane slabosti. Zavedati se moramo, da se vsakodnevno soočamo s kibernetskimi grožnjami in ranljivostmi informacijsko komunikacijskih sistemov, ki bi v primeru realizacije lahko imeli težko popravljive posledice za državo in gospodarstvo. V času Predsedovanja Svetu EU v drugi polovici leta 2021 smo pred izzivom zagotavljanja razpoložljivosti, dostopnosti in zaupnosti informacijsko komunikacijskih sistemov povezanih s predsedovanjem. Kibernetsko varno predsedovanje bo ključno za ugled države. Tudi v ta namen moramo dvigniti nivo odpornosti. Zato je nujna čimprejšnja ustrezna umestitev pristojnega nacionalnega organa, ki mora takoj prevzeti proaktivno vlogo na področju informacijsko kibernetske varnosti.

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- dr. Uroš Svete, direktor uprave, Uprava Republike Slovenije za informacijsko varnost,
- Kory Golob, vodja Sektorja za strateško načrtovanje in krizno odzivanje, Uprava Republike Slovenije za informacijsko varnost,
- Matjaž Mravljak, vodja inšpekcije, Inšpektorat za Informacijsko družbo, Uprava Republike Slovenije za informacijsko varnost.

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:

- Boštjan Koritnik, minister za javno upravo,
- mag. Peter Geršak, državni sekretar na Ministrstvu za javno upravo,
- dr. Uroš Svete, direktor uprave, Uprava Republike Slovenije za informacijsko varnost.

5. Kratek povzetek gradiva:

Spreminja se umestitev pristojnega nacionalnega organa za informacijsko varnost po Zakonu o informacijski varnosti. Uprava Republike Slovenije za informacijsko varnost, organ v sestavi Ministrstva za javno upravo se preoblikuje v samostojno vladno službo. V novo vladno službo se umesti tudi CSIRT organov državne uprave, skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov. Z novo umestitvijo se bo doseglo dvig nivoja koordinacije kibernetske varnosti ter doseglo primerljivo ureditev z vodilnimi državami.

6. Presoja posledic za:

a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	**DA**/NE
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	DA/**NE**
c)	administrativne posledice	DA/**NE**

č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	DA/**NE**
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	DA/**NE**
e)	socialno področje	DA/**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	DA/**NE**

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:

Predlog sprememb in dopolnitev Zakona o informacijski varnosti ima finančne posledice za državni proračun, ki izhajajo predvsem iz naslova vzpostavitve samostojne vladne strokovne službe. V aktu o notranji organizaciji in sistemizaciji delovnih mest bo potrebno sistemizirati posebna delovna mesta za izvajanje nalog na področju upravljanja kadrovskih, finančnih, informacijskih in drugih virov ter zagotoviti kadrovsko popolnitev. Predvideva se, da bi omenjene naloge opravljali trije novi javni uslužbenci.

Prav tako je potrebno upoštevati finančne posledice vzpostavitve CSIRT organov državne uprave v okviru samostojne strokovne službe. Upoštevana je projekcija, ki je bila narejena že ob sprejemu Zakona o informacijski varnosti leta 2018, ki predvideva, da bodo naloge CSIRT organov državne uprave v letu 2021 opravljali štirje javni uslužbenci.

Finančne posledice za državni proračun so ocenjene na 385.000 eurov letno in se zagotovijo iz veljavnega proračuna Uprave Republike Slovenije za informacijsko varnost za leto 2021.

Predlog zakona nima finančnih posledic za druga javna finančna sredstva.

Pri pripravi kadrovskih načrtov se bo sledilo restriktivnim določbam politike zaposlovanja iz 60. člena Zakona o izvrševanju proračunov za leti 2021 in 2022 - ZIPRS2122, v katerem je med drugim opredeljeno, na podlagi katerih utemeljenih razlogov je organu dovoljeno (izjemoma) povečati število zaposlenih.

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
3132 Uprava RS za informacijsko varnost	3132-20-0001 Delovanje Uprave RS za informacijsko varnost	200038 Plače	130.000	260.000
3132 Uprava RS za informacijsko varnost	3132-20-0001 Delovanje Uprave RS za informacijsko varnost	200039 Materialni stroški	12.500	25.000
3132 Uprava RS za informacijsko varnost	3132-20-0003 Investicije in investicijsko vzdrževanje URSIV	200040 Investicije in investicijsko vzdrževanje	50.000	100.000
SKUPAJ			192.500	385.000

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:

I. 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.

II. 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/**NE**

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: DA/**NE**
- Združenju občin Slovenije ZOS: DA/**NE**
- Združenju mestnih občin Slovenije ZMOS: DA/**NE**

Predlogi in pripombe združenj so bili upoštevani:

- v celoti,
- večinoma,
- delno,
- niso bili upoštevani.

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: **NE**
- Združenju občin Slovenije ZOS: **NE**
- Združenju mestnih občin Slovenije ZMOS: **NE**

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/**NE**
10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	DA/**NE**
11. Gradivo je uvrščeno v delovni program vlade:	DA/**NE**
Boštjan Koritnik minister Priloge: – predlog sklepa vlade – predlog zakona – predlog uredbe 2x	

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 in 55/17) je Vlada Republike Slovenije na ..... seji dne ..... pod točko ..... sprejela sklep:

Vlada Republike Slovenije je določila besedilo predloga Zakona o spremembah in dopolnitvi Zakona o informacijski varnosti (EVA 2021-3130-0020) in ga pošlje v obravnavo Državnemu zboru Republike Slovenije po nujnem postopku.

mag. Janja Garvas Hočevar
vršilka dolžnosti generalnega
sekretarja

Priloga:
- besedilo predloga zakona.

Prejmejo:
- Državni zbor Republike Slovenije,
- Ministrstvo za javno upravo,
- Ministrstvo za finance,
- Ministrstvo za obrambo,
- Ministrstvo za notranje zadeve,
- Služba Vlade Republike Slovenije za zakonodajo.

PRILOGA 3 (jedro gradiva)

PREDLOG
(EVA 2021-3130-0020)

PREDLOG ZAKONA O SPREMEMBAH IN DOPOLNITVI 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.

Aprila 2018 je Državni zbor Republike Slovenije sprejel Zakon o informacijski varnosti (Uradni list RS št. 30/18; v nadaljevanju: ZInfV), ki je začel veljati 11. 5. 2018. ZInfV postavlja sistemsko ureditev področja informacijske/kibernetske 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. ZInfV med drugim ureja tudi organizacijo nacionalnega sistema informacijske/kibernetske varnosti.

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

Pristojni nacionalni organ za informacijsko varnost (v nadaljevanju: PNO), ki ga uvaja ZInfV, je začel delovati 1. 1. 2020 (prehodna določba 40. člena ZInfV). Do začetka delovanja PNO je njegove naloge v skladu z ZInfV opravljal Urad Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljevanju: UVTP), razen nalog upravnega odločanja in nadzora, ki jih je opravljalo ministrstvo, pristojno za informacijsko družbo. Uredba o spremembah in dopolnitvah Uredbe o organih v sestavi ministrstev (Uradni list RS, št. 52/18) v skladu s prvim odstavkom 27. člena ZInfV določa, da je PNO organ v sestavi ministrstva, pristojnega za informacijsko družbo. V okviru obstoječe razmejitve resornih pristojnosti ministrstev je določila, da je PNO Uprava Republike Slovenije za informacijsko varnost (v nadaljevanju URSIV), organ v sestavi Ministrstva za javno upravo (v nadaljevanju: MJU). URSIV opravlja svoje naloge v naslednjih organizacijskih enotah: Sektorju za skupne zadeve, Sektorju za dvig odpornosti, Sektorju za strateško načrtovanje in krizno odzivanje ter Inšpekciji za informacijsko družbo.

URSIV je osrednji koordinacijski organ na strateški ravni nacionalnega sistema zagotavljanja informacijske varnosti, obenem pa je tudi enotna kontaktna točka države pri mednarodnem sodelovanju na tem področju. Na podlagi tretjega odstavka 9. člena Uredbe o organih v sestavi ministrstev (Uradni list RS, št. 35/15, 62/15, 84/16, 41/17, 53/17, 52/18, 84/18, 10/19, 64/19 in 64/21) URSIV:

- odloča o sprejemu ukrepov ob težjem ali kritičnem incidentu ali kibernetskem napadu kot tudi stanju povečane ogroženosti;
- odloča v postopkih nadzora v skladu z zakonom, ki ureja informacijsko varnost;
- vodi seznam kontaktnih podatkov zavezancev ter skupni seznam incidentov in kibernetskih napadov;
- obvešča javnost o incidentih in v zvezi z njimi sprejetih ukrepih;
- izpolnjuje mednarodne obveznosti in opravlja naloge mednarodne izmenjave podatkov vključno z izvajanjem nalog enotne kontaktne točke in sodelovanjem s pristojnimi organi s področja informacijske varnosti v Evropski uniji, določene z zakonom, ki ureja informacijsko varnost;
- opravlja koordinacijske, strokovno tehnične, organizacijske in razvojne naloge na področju informacijske varnosti in kibernetske obrambe, določene z zakonom, ki ureja informacijsko varnost, in njegovimi podzakonskimi predpisi;
- izvaja naloge spremljanja in poročanja na podlagi zakona, ki ureja dostopnost spletišč in mobilnih aplikacij;
- odloča v postopkih nadzora skladno z zakonom, ki ureja dostopnost spletišč in mobilnih aplikacij;
- opravlja naloge inšpekcijskega nadzora na področju elektronske identifikacije, storitev zaupanja ter naloge vodenja nacionalnega zanesljivega seznama ponudnikov kvalificiranih storitev zaupanja.

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

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).

Državni zbor Republike Slovenije je v Resoluciji o strategiji nacionalne varnosti Republike Slovenije (Uradni list RS, št. 59/19) informacijsko-kibernetske grožnje opredelil kot eno ključnih groženj. Svet za nacionalno varnost (SNAV) je na seji 4. 5. 2020 sklenil, da Slovenija potrebuje skupen in celovit pristop na področju kibernetske varnosti. V okviru predsedovanja Svetu EU v drugi polovici leta 2021 je za eno od strateških tem določena digitalizacija, znotraj nje pa kot prioritetno vprašanje ravno kibernetska varnost.

Vlada Republike Slovenije se je na 198. dopisni seji 9. 4. 2021 seznanila z informacijo o ustanovitvi in imenovanju Strateškega sveta za digitalizacijo, ki je posvetovalno telo predsednika

vlade. Naloge Strateškega sveta so, da za predsednika vlade v petih mesecih pripravi okvirni predlog potrebnih sistemskih sprememb za pospešitev digitalizacije slovenskega gospodarstva, javnega sektorja in državne uprave; pripravlja mnenja k vprašanjem, pobudam ali predlogom povezanih z digitalizacijo gospodarstva, javne uprave in družbe kot celote; za predsednika vlade pripravlja mnenja in predloge glede strategije razvoja umetne inteligence, kibernetske varnosti in drugih področij delovnega področja sveta; spremljanje izvedbe strategij, načrtov in ukrepov na področju digitalizacije (Digitalna Slovenija, Strategija razvoja javne uprave...); spremljanje globalnega razvoja digitalnih tehnologij in priprava strateških usmeritev; predsedniku vlade predlaga konkretne ukrepe in pravne akte s področja digitalizacije. Ob odločitvi za pospešitev procesa digitalizacije slovenske družbe je treba nameniti ustrezno pozornost kibernetski varnosti in s tem grožnjam kibernetskih napadov. Ti so sestavni del digitalne dobe. Za ustrezno odzivanje potrebuje Republika Slovenija ureditev kibernetske varnosti, ki je primerljiva najbolj uspešnim evropskim državam.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji

Cilj predloga zakona je sistemsko urediti in nadgraditi področje informacijske varnosti tako na strateški kot tudi na operativni ravni nacionalnega sistema zagotavljanja informacijske varnosti.

Zato se določa, da pristojni nacionalni organ za informacijsko varnost deluje kot samostojna strokovna služba Vlade Republike Slovenije. Direktorja urada imenuje in razrešuje Vlada Republike Slovenije na predlog predsednika vlade. Direktor je za delo urada neposredno odgovoren predsedniku vlade. Urad z lastno inšpekcijsko službo izvaja nadzor nad izvajanjem ZInfV ter pripravlja predloge predpisov s področja informacijske in kibernetske varnosti za Vlado Republike Slovenije.

Nadzor nad skladnostjo spletišč in mobilnih aplikacij po Zakonu o dostopnosti spletišč in mobilnih aplikacij (Uradni list RS, št. 30/18) ter nadzor na področju e-identitet in storitev zaupanja izvaja pristojna inšpekcija Ministrstva za javno upravo.

2.2 Načela

Predlog zakona ne odstopa od načel, ki so bila upoštevana že ob pripravi veljavnega zakona. Upoštevana so zlasti načela ustavnosti, zakonitosti, enakosti in sorazmernosti.

2.3 Poglavitne rešitve

Predlagane spremembe in dopolnitve Zakon o informacijski varnosti prinašajo naslednje rešitve:

- Z namenom okrepitve strateške in operativne ravni se Uprava Republike Slovenije za informacijsko varnost, organ v sestavi MJU preoblikuje v samostojno strokovno službo Vlade Republike Slovenije.
- Sestavni del omenjene službe je tudi skupina za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (CSIRT organov državne uprave), ki sedaj deluje v okviru MJU.

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

Predlog sprememb in dopolnitev Zakona o informacijski varnosti ima finančne posledice za državni proračun, ki izhajajo predvsem iz naslova vzpostavitve samostojne vladne strokovne službe. V aktu o notranji organizaciji in sistemizaciji delovnih mest bo potrebno sistemizirati posebna delovna mesta za izvajanje nalog na področju upravljanja kadrovskih, finančnih, informacijskih in drugih virov ter zagotoviti kadrovsko popolnitev. Predvideva se, da bi omenjene naloge opravljali trije novi javni uslužbenci.

Prav tako je potrebno upoštevati finančne posledice vzpostavitve CSIRT organov državne uprave v okviru samostojne strokovne službe. Upoštevana je projekcija, ki je bila narejena že ob sprejemu Zakona o informacijski varnosti leta 2018, ki predvideva, da bodo naloge CSIRT organov državne uprave v letu 2021 opravljali štirje javni uslužbenci.

Finančne posledice za državni proračun so ocenjene na 385.000 eurov letno in se zagotovijo iz veljavnega proračuna Uprave Republike Slovenije za informacijsko varnost za leto 2021. Finančna sredstva so zagotovljena pri proračunskem uporabniku 3132 Uprava RS za informacijsko varnost:

- šifra in naziv ukrepa, projekta: 3132-20-0001 »Delovanje Uprave RS za informacijsko varnost«, šifra in naziv proračunske postavke: 200038 »Plače«;
- šifra in naziv ukrepa, projekta: 3132-20-0001 »Delovanje Uprave RS za informacijsko varnost«, šifra in naziv proračunske postavke: 200039 »Materialni stroški«;
- šifra in naziv ukrepa, projekta: 3132-20-0001 »Investicije in investicijsko vzdrževanje URSIV«, šifra in naziv proračunske postavke: 200040 »Investicije in investicijsko vzdrževanje«.

Predlog zakona nima finančnih posledic za druga javna finančna sredstva.

Pri pripravi kadrovskih načrtov se bo sledilo restriktivnim določbam politike zaposlovanja iz 60. člena Zakona o izvrševanju proračunov za leti 2021 in 2022 - ZIPRS2122, v katerem je med drugim opredeljeno, na podlagi katerih utemeljenih razlogov je organu dovoljeno (izjemoma) povečati število zaposlenih.

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

Sredstva za izvajanje zakona v letu 2021 so zagotovljena v državnem proračunu za leto 2021.

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

Republika Avstrija

Za področje kibernetske varnosti so v Avstriji pristojni Zvezno kanclerstvo (Bundeskanzleramt – BKA), Zvezno ministrstvo za notranje zadeve (Bundesministerium für Inneres – BMI), Zvezno ministrstvo za evropske in mednarodne zadeve (Bundesministerium für europäische und internationale Angelegenheiten – BMEIA) in Zvezno ministrstvo za narodno obrambo (Bundesministerium für Landesverteidigung – BMLV). Zvezno kanclerstvo usklajuje nacionalna in mednarodna strateška vprašanja kibernetske varnosti in sodeluje v različnih delovnih telesih z nacionalnimi, evropskimi in mednarodnimi akterji. Vodi tudi rezervni računalniški center zvezne

vlade (das Ausweichrechenzentrum des Bundes – ZAS) in vladni odzivni center za kibernetsko varnost (GovCERT Austria).

Češka republika

V Češki republiki je v skladu z odločbo češke vlade št. 781 z dne 19. oktobra 2011 za zagotavljanje kibernetske varnosti odgovoren Nacionalni varnostni organ (v nadaljnjem besedilu: NVO). Z isto odločbo sta bila ustanovljena tudi Nacionalni center za kibernetsko varnost (v nadaljnjem besedilu: NCKV), ki je podrejen NVO, in Svet za kibernetsko varnost (v nadaljnjem besedilu: SKV). NCKV upravlja vladni CERT, usmerja sodelovanje s skupinami CSIRT tako na nacionalni kot tudi mednarodni ravni, pripravlja varnostne standarde za različne kategorije subjektov v državi, podpira izobraževanje in dvig ozaveščenosti o kibernetski varnosti ter podpira raziskave in razvoj na področju kibernetske varnosti. NVO nadzira in redno ocenjuje delo NCKV, njegovo letno poročilo pa prouči tudi SKV in potrdi vlada.

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

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. ANSSI je naslednica Centralnega direktorata za varnost omrežij in informacij (Central Directorate for Network and Information Security – DCSSI) Generalnega sekretariata za nacionalno obrambo (secrétariat général de la défense nationale – SGDN). Generalnega direktorja ANSSI z odlokom imenuje predsednik vlade. Slednji ANSSI kot nacionalni organ poroča generalnemu sekretarju za obrambo in nacionalno varnost (SGDSN). Svetuje predsedniku vlade pri izpolnjevanju njegovih nalog v zvezi z nacionalno obrambo in varnostjo. Kot pristojni nacionalni organ za kibernetsko obrambo ter varnost omrežij in informacij v skladu z direktivo (NIS) ANSSI ponuja 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 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.

6. PRESOJA POSLEDIC, KI JIH BO IMEL SPREJEM ZAKONA

6.1 Presoja administrativnih posledic:

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

Sprejetje zakona prinaša učinkovitejše delo na področju koordinacije kibernetske varnosti.

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

Zakon 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:

Zakon ne bo imel posledic na okolje.

6.3 Presoja posledic za gospodarstvo:

Zakon ne bo imel posledic na gospodarstvo.

6.4 Presoja posledic za socialno področje:

Zakon ne bo imel posledic na socialnem področju.

6.5 Presoja posledic za dokumente razvojnega načrtovanja:

Zakon ne bo imel posledic pri dokumentih razvojnega načrtovanja.

6.6 Presoja posledic za druga področja:

Zakon ne bo imel posledic na drugih področjih.

6.7 Izvajanje sprejetega predpisa:

Zakon bo predstavljen članom Koordinacijske skupine za kibernetsko varnost, izvajalcem bistvenih storitev in organom državne uprave.

Izvajanje tega zakona bo spremljal pristojni nacionalni organ za informacijsko varnost. Metodologija za spremljanje doseganja ciljev ni predvidena.

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:

Predlog zakona se obravnava po nujnem postopku. Predlog zakona ureja le notranjo organizacijo državnih organov, zato javnost ni sodelovala pri njegovi pripravi.

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. Prav tako niso sodelovale pravne osebe.

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

- Boštjan Koritnik, minister za javno upravo,
- mag. Peter Geršak, državni sekretar na Ministrstvu za javno upravo,
- dr. Uroš Svete, direktor uprave, Uprava Republike Slovenije za informacijsko varnost.

II. BESEDILO ČLENOV

1. člen

V Zakonu o informacijski varnosti (Uradni list RS, št. 30/18) se v 12. členu v tretjem odstavku besedilo »Minister, pristojen za informacijsko družbo (v nadaljnjem besedilu: minister)« nadomesti z besedo »Vlada«.

2. člen

V 17. členu se v tretjem odstavku beseda »Minister« nadomesti z besedo »Vlada«.

3.člen

V 25. členu se v petem odstavku za besedilom »in organov državne uprave« doda besedilo »ter odzivanja na incidente in kibernetske napade«.

4. člen

V 26. členu se v naslovu beseda »informacijske« nadomesti z besedo »kibernetske«.

V prvem odstavku se v prvem stavku se besedilo »strategijo informacijske« nadomesti z besedilom »strategijo kibernetske«, za besedilom »zagotavljanja informacijske« pa se doda besedilo »oziroma kibernetske«.

5. člen

V 27. členu se prvi odstavek spremeni tako, da se glasi:

»(1) Pristojni nacionalni organ je Urad Vlade Republike Slovenije za informacijsko varnost.«.

V drugem odstavku se na koncu 16. točke pika nadomesti s podpičjem in se dodata novi 17. in 18. točka, ki se glasita:

»17. pripravlja predloge predpisov s področja informacijske in kibernetske varnosti;
18. izvaja naloge nacionalnega certifikacijskega organa za kibernetsko varnost.«.

6. člen

V 29. členu se prvi odstavek spremeni tako, da se glasi:

»(1) Naloge CSIRT organov državne uprave izvaja pristojni nacionalni organ.«.

7. člen

V 31. členu se četrti odstavek spremni tako, da se glasi:
»(4) Zoper odločbo, izdano v postopkih nadzora po tem zakonu, 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.”.

8. člen

V 32. členu se v tretjem odstavku črta besedilo »ki jo je izvajalec bistvenih storitev pripravil skupaj s pristojnim nacionalnim organom, ali ocena varnosti,«.

9. člen

V tretjem odstavku 34. člena se v tretjem odstavku črta besedilo »ki jo je organ državne uprave pripravil skupaj s pristojnim nacionalnim organom, ali ocena varnosti,«.

PREHODNE IN KONČNA DOLOČBA

10. člen
(začetek delovanja vladne službe)

(1) Vlada Republike Slovenije ustanovi urad iz prvega odstavka 27. člena zakona v enem mesecu od uveljavitve tega zakona. Urad začne opravljati naloge v skladu s tem zakonom najpozneje do 31. julija 2021, do takrat pa njegove naloge opravlja Uprava Republike Slovenije za informacijsko varnost, organ v sestavi ministrstva, pristojnega za informacijsko družbo.

(2) Urad iz prejšnjega odstavka z začetkom delovanja od ministrstva, pristojnega za informacijsko družbo prevzame naloge, arhive in dokumentacijo, ki se nanašajo na informacijsko varnost, ter javne uslužbence, pravice proračunske porabe, opremo in druge zbirke podatkov oziroma evidence s prevzetega delovnega področja.

(3) Upravni in inšpekcijski postopki, začeti na podlagi Zakona o informacijski varnosti (Uradni list RS, št. 30/18), se dokončajo v skladu z določbami tega zakona.

11. člen
(delovanje drugih pristojnih organov)

(1) CSIRT organov državne uprave se vzpostavi pri pristojnem nacionalnem organu do 1. januarja 2022.

(2) Do vzpostavitve CSIRT organov državne uprave pri pristojnem nacionalnem organu njegove naloge opravlja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave.

12. člen
(izdaja podzakonskih predpisov in strategije)

(1) Vlada Republike Slovenije uskladi Uredbo o organih v sestavi ministrstev (Uradni list RS, št. 35/15, 62/15, 84/16, 41/17, 53/17, 52/18, 84/18, 10/19, 64/19 in 64/21) s tem zakonom v treh mesecih od njegove uveljavitve.

(2) Vlada Republike Slovenije izda predpisa iz tretjega odstavka 12. člena in tretjega odstavka 17. člena zakona v enem letu od uveljavitve tega zakona.

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

13. člen
(prenehanje veljavnosti in podaljšanje uporabe)

Z dnem uveljavitve tega zakona prenehata veljati Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 32/19) ter Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 68/19), ki pa se uporabljata do izdaje podzakonskih predpisov iz drugega odstavka prejšnjega člena.

14. člen
(Zakon o dostopnosti spletišč in mobilnih aplikacij)

(1) V Zakonu o dostopnosti spletišč in mobilnih aplikacij (Uradni list RS, št. 30/18) se v 10. členu za besedo »inšpektorji« doda besedilo »organa, pristojnega«.

(2) V 11. členu se v prvem, drugem in petem odstavku beseda »varnost« nadomesti z besedo »družbo«.

15. člen
(začetek veljavnosti)

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

III. OBRAZLOŽITEV

K 1. členu:
Gre za popravek oziroma spremembo, ki je posledica nove organizacijske oblike pristojnega nacionalnega organa.

K 2. členu:
Gre za popravek oziroma spremembo, ki je posledica nove organizacijske oblike pristojnega nacionalnega organa.

K 3. členu:
Dopolnitev člena ureja namen vodenja seznama tudi za odzivanje na incidente ter kibernetske napade. Dosedanja ureditev je obsegala le namen določitve. V praksi se je izkazalo, da pristojni nacionalni organ za ustrezno odzivanje potrebuje informacijo o informacijskih sistemih, delih omrežja in informacijskih storitvah zavezancev.

K 4. členu:
Člen ureja redakcijski popravek in uskladitev s 4. členom (pomen izrazov) Zakona o informacijski varnosti (Uradni list RS, št. 30/18), ki v 37. točki določa pomen izraza »Strategija kibernetske varnosti«. Z izrazom razumemo nacionalno strategijo za varnost omrežij in informacijskih sistemov ter pomeni okvir s strateškimi cilji in prednostnimi nalogami na področju varnosti omrežij in informacijskih sistemov v Republiki Sloveniji. Z ureditvijo izrazoslovja bosta dosežena terminološka konsistentnost in časovna vez z veljavno Strategijo kibernetske varnosti, ki jo je Vlada Republike Slovenije sprejela leta 2016.

K 5. členu:
Z vzpostavitvijo pristojnega nacionalnega organa kot samostojne strokovne službe vlade se nadaljuje proces sistemskega urejanja in nadgradnje področja informacijske varnosti na strateški ravni nacionalnega sistema zagotavljanja informacijske varnosti. Gre za rešitev, ki je primerljiva z najbolj naprednimi evropskimi državami na področju kibernetske varnosti. Z vpeljavo strateškega organa na vladnem nivoju se tudi simbolično daje pomen kibernetske varnosti kot pomembnemu segmentu pospešene digitalizacije slovenske družbe. Upoštevati je treba, da je oziroma bo pristojni nacionalni organ prevzel nove naloge na področju certifikacije in nacionalnega koordinacijskega centra za industrijo, tehnologijo in raziskave na področju kibernetske varnosti.

Ureja se tudi področje priprave predlogov predpisov (zakonov in podzakonskih predpisov) s področja informacijske in kibernetske varnosti. Pristojni nacionalni organ bo omenjeno nalogo vključil v proces koordinacije kibernetske varnosti, ki jo stalno izvaja na podlagi Nacionalnega načrta odzivanja na kibernetske incidente, ki ga je Vlada Republike Slovenije sprejela marca 2021.

K 6. členu:
Na pristojni nacionalni organ se prenesejo naloge CSIRT organov državne uprave. CSIRT je skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize na strateški ravni in pomaga priglasiteljem pri obvladovanju težjih incidentov. Gre za rešitev, ki je primerljiva z najbolj naprednimi evropskimi državami na področju kibernetske varnosti, pri katerih je CSIRT organov državne uprave organiziran kot enota pristojnega nacionalnega organa.

K 7. členu:
Veljavna določba člena navaja samo organ vložitve tožbe zoper dokončno odločbo in nujnost ter prednost postopka. Določba je nejasna v smislu ali je dopustna pritožba na dokončno odločbo, izdano v postopkih izvajanja nadzora. Predlagana dopolnitev jasno in nedvoumno določa pravno sredstvo in način vložitve pravnega sredstva zoper dokončno odločbo, izdano v postopkih nadzora po tem zakonu.

K 8. členu:
Gre za popravek oziroma spremembo, ki nedvoumno ureja področje revizije ocene varnosti omrežij in informacijskih sistemov. Z rešitvijo, ki predvideva, da oceno varnosti lahko pripravi le kvalificirani revizor, bo doseženo poenotenje postopkov in rezultatov.

K 9. členu:
Gre za popravek oziroma spremembo, ki nedvoumno ureja področje revizije ocene varnosti omrežij in informacijskih sistemov. Z rešitvijo, ki predvideva, da oceno varnosti lahko pripravi le kvalificirani revizor, bo doseženo poenotenje postopkov in rezultatov.

K 10. členu:
Člen določa ustanovitev in začetek delovanja pristojnega nacionalnega organa kot Urada Vlade Republike Slovenije za informacijsko varnost (samostojne strokovne službe vlade), ki začne z delovati najpozneje do 31. julija 2021. V prehodnem obdobju opravlja naloge Uprava Republike Slovenije za informacijsko varnost, organ v sestavi Ministrstva za javno upravo (ministrstva, pristojnega za informacijsko družbo). Določbe člena določajo prevzem nalog, arhivov in dokumentacije, ki se nanašajo na informacijsko varnost, ter javnih uslužbencev, pravic proračunske porabe, opreme in drugih zbirk podatkov oziroma evidenc s prevzetega delovnega področja Uprave Republike Slovenije za informacijsko varnost, ki bo ukinjena z ustanovitvijo Urada Vlade Republike Slovenije za informacijsko varnost. Začeti upravni in inšpekcijski postopki v Upravi Republike Slovenije za informacijsko varnost na podlagi Zakona o informacijski varnosti, se nadaljujejo v inšpekcijskem organu Urada Vlade Republike Slovenije za informacijsko varnost.

K 11. členu:
Člen določa rok za vzpostavitev CSIRT organov državne uprave pri pristojnem nacionalnem organu, in sicer do 1. januarja 2022 ter prehodno obdobje, v katerem njegove naloge še vedno opravlja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave.

K 12. členu:
Člen določa rok za izdajo Odloka o organizaciji in delovnem področju samostojne strokovne službe, uskladitve Uredbe o organih v sestavi ministrstev (Uradni list RS, št. 35/15, 62/15, 84/16, 41/17, 53/17, 52/18, 84/18, 10/19, 64/19 in 64/21)

K13. členu:
Člen določa prenehanje veljavnosti Pravilnika o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (Uradni list RS, št. 32/19) in Pravilnika o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 68/19) in podaljšanje uporabe do izdaje podzakonskih predpisov iz drugega odstavka prejšnjega člena. Z rešitvijo se izognemo pravni praznini.

K 14. členu:
Formalno se spreminja pristojnost opravljanja inšpekcijskega nazora nad izvajanjem določb Zakona o dostopnosti spletišč in mobilnih aplikacij (Uradni list RS, št. 30/18). Trenutno opravlja inšpekcijski nadzor nad izvajanjem določb tega zakona Inšpekcija za informacijsko družbo v Upravi Republike Slovenije za informacijsko varnost. Zaradi predlagane spremembe Zakona o informacijski varnosti in posledično drugačne formalne umestitve in nalog Uprave Republike Slovenije za informacijsko varnost kot nacionalnega pristojnega organa za informacijsko (kibernetsko) varnost (sedaj organa v sestavi v Ministrstvu za javno upravo, po spremembi pa kot samostojna vladna služba) se spreminja delovno področje uprave, ki se bo ukvarjala izključno z informacijsko (kibernetsko) varnostjo, inšpekcijski nadzor nad izvajanjem tega zakona pa bo še naprej opravljal organ v Ministrstvu za javno upravo, kot ministrstvo, pristojno za informacijsko družbo.
Posledično se zaradi spremembe 10. člena Zakona o dostopnosti spletišč in mobilnih aplikacij spreminja poimenovanje organa za spremljanje in poročanje, ko to ne bo več Uprava Republike Slovenije za informacijsko varnost ampak bo to opravljal organ v Ministrstvu za javno upravo, kot ministrstvo, pristojno za informacijsko družbo.

K 15. členu:
Določa se začetek veljavnosti zakona, to je naslednji dan po objavi v Uradnem listu Republike Slovenije. Izkazana je nujnost določitve krajše »vacatio legis« od običajne zaradi čim hitrejše izdaje s spremembo povezanih izvršilnih predpisov in aktov o ustanovitvi Urada Vlade Republike Slovenije za informacijsko varnost ter čim krajšim prehodnim obdobjem zaradi ustreznega prenosa nalog, arhivov in dokumentacije, ki se nanašajo na informacijsko varnost, ter javnih uslužbencev, pravic proračunske porabe, opreme in drugih zbirk podatkov oziroma evidenc iz prevzetega delovnega področja Uprave Republike Slovenije za informacijsko varnost.

IV. BESEDILO ČLENOV, KI SE SPREMINJAJO
(prepis določb veljavnega zakona, ki se s predlogom spreminjajo)

Zakon o informacijski varnosti (Uradni list RS, št. 30/18)

12. člen
(varnostna dokumentacija in varnostni ukrepi)

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

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

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

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

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

17. člen
(varnostna dokumentacija in varnostni ukrepi)

(1) Organi državne uprave za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov državnih organov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj:
1. analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj,
2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja,
3. seznam informacijskih sistemov in delov omrežja organov državne uprave ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev organov državne uprave,

4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje,
5. načrt odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave in
6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov organov državne uprave.

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

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

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

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

25. člen
(vodenje in vsebina seznamov)

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

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

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

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

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

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

26. člen
(strategija informacijske varnosti)

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

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

27. člen
(pristojni nacionalni organ)

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

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

1. koordinira delovanje sistema informacijske varnosti;
2. razvija zmogljivosti za izvajanje kibernetske obrambe;
3. vsem zavezancem pri izvajanju njihovih nalog nudi strokovno podporo na področju informacijske varnosti;
4. zagotavlja analize, metodološko podporo in preventivno delovanje na področju informacijske varnosti ter daje mnenja s področja svojih prisotnosti;
5. sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, predvsem z nacionalnim CSIRT in CSIRT organov državne uprave, z varnostno-operativnimi centri, z regulatorji oziroma nadzorniki področij iz drugega odstavka 5. člena, z Agencijo za komunikacijska omrežja in storitve Republike Slovenije, z Informacijskim pooblaščencem in z organi kazenskega pregona ter s ponudniki varnostnih rešitev;
6. zavezance ozavešča o pomembnosti prijave incidenta z vsemi znaki kaznivega dejanja, ki se preganja po uradni dolžnosti, organom kazenskega pregona, skladno s Kazenskim zakonikom;
7. koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za dvig zavedanja javnosti o informacijski varnosti;
8. spodbuja in podpira raziskave in razvoj na področju informacijske varnosti;
9. izvaja testiranja informacijsko-komunikacijskih tehnologij na področju informacijske varnosti;
10. skrbi za pripravo in izvajanje strategije;
11. izdela nacionalni načrt odzivanja na incidente ob upoštevanju strategije, načrtov nacionalnega CSIRT in CSIRT organov državne uprave, drugih pristojnih organov ter varnostne dokumentacije zavezancev;

12. pregleduje ustreznost določitve izvajalcev bistvenih storitev in organov državne uprave vsaj vsaki dve leti ter vladi lahko predlaga posodobitev določitev;
13. za namene pregleda Direktive 2016/1148/ES Evropsko komisijo vsaj vsaki dve leti obvešča o ukrepih za določitev storitev izvajalcev bistvenih storitev, njihovem številu ter pomenu, o seznamu bistvenih storitev ter pragih za določitev ustrezne ravni opravljanja storitev izvajalcev bistvenih storitev glede na število uporabnikov ali glede na pomen zadevnega izvajalca bistvenih storitev;
14. je enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU ter z mrežo skupin CSIRT in s skupino za sodelovanje, v katero prispeva svojega predstavnika;
15. izpolnjuje druge obveznosti obveščanja Evropske komisije in skupine za sodelovanje, obveznosti obveščanja in notifikacije preostalih mednarodnih organizacij;
16. izvaja druge naloge mednarodnega sodelovanja.

29. člen
(CSIRT organov državne uprave)

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

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

31. člen
(pristojnost, postopek in pravna sredstva)

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

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

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

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

32. člen
(nadzor nad izvajalci bistvenih storitev)

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

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

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

34. člen
(nadzor nad organi državne uprave)

(1) Inšpektor nadzira, ali organi državne uprave izpolnjujejo svoje obveznosti iz prvega in drugega odstavka 16. člena, iz prvega, drugega in petega odstavka 17. člena, iz prvega in drugega odstavka 18. člena tega zakona ter iz odločb, izdanih na podlagi četrtega odstavka 21. člena in četrtega odstavka 22. člena tega zakona, ter na njihovi podlagi določene ukrepe za varnost omrežij in informacijskih sistemov.

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

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

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

Zakon o dostopnosti spletišč in mobilnih aplikacij (Uradni list RS, št. 30/18)

10. člen
(inšpekcijski nadzor)

Nadzor nad izvajanjem določb 5. do 8. člena tega zakona opravljajo inšpektorji za informacijsko družbo.

11. člen
(spremljanje in poročanje)

(1) Organ, pristojen za informacijsko varnost, redno spremlja skladnost spletišč in mobilnih aplikacij z zahtevami glede dostopnosti iz 5. člena tega zakona.

(2) Organ, pristojen za informacijsko varnost, vsako tretje leto poroča Evropski komisiji o rezultatih spremljanja, vključno s podatki merjenja. Poročilo vsebuje tudi informacije o opravljenih inšpekcijskih nadzorih iz prejšnjega člena.

(3) Prvo poročilo poleg podatkov iz prejšnjega odstavka obsega tudi:
- opis mehanizmov za posvetovanje z ustreznimi udeleženci o dostopnosti spletišč in mobilnih aplikacij,
- postopke za objavo vseh informacij o razvoju politike dostopnosti v zvezi s spletišči in mobilnimi aplikacijami,
- izkušnje in ugotovitve, zbrane med izvajanjem tega zakona v zvezi s skladnostjo z zahtevami glede dostopnosti iz 5. člena tega zakona in
- informacije o dejavnostih usposabljanja in ozaveščanja.

(4) Če pride do bistvenih sprememb informacij iz prejšnjega odstavka, naslednja poročila vsebujejo tudi informacije v zvezi s temi spremembami.

(5) Organ, pristojen za informacijsko varnost, vsebino poročil, brez seznama pregledanih spletišč, mobilnih aplikacij ali zavezancev, objavi na svojih spletnih straneh, pri čemer upošteva zahteve iz 5. člena tega zakona.

(6) Minister določi metodologijo za spremljanje iz prvega odstavka tega člena.

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

Predlaga se nujni postopek obravnave predloga zakona v Državnem zboru Republike Slovenije na podlagi prvega odstavka 143. člena Poslovnika državnega zbora (Uradni list RS, št. 92/07 – uradno prečiščeno besedilo, 105/10, 80/13,38/17 in 46/20), ker je sprejem zakona nujen zaradi interesov varnosti države in da se preprečijo težko popravljive posledice za delovanje države.

Veljavni Zakon o informacijski varnosti (Uradni list RS, št. 30/18) določa umestitev pristojnega nacionalnega organa kot organ v sestavi Ministrstva za javno upravo.

Nacionalne in mednarodne izkušnje kažejo, da so pristojni nacionalni organi za področje informacijske (kibernetske) varnosti postali ključni deležniki v sistemu zagotavljanja nacionalne varnosti sodobnih držav. Zavedati se moramo, da je digitalizacija vseprisotna, za njen razvoj se bo namenjalo vedno več sredstev, širila se bo v vse družbene podsisteme, treba pa bo zagotavljati visoko stopnjo informacijske varnosti.

Nujno je treba vzpostaviti čimprejšnje mednarodne izmenjave podatkov v mreži CSIRT in okrepiti mednarodno sodelovanje med nacionalnimi organi. Pri obravnavi zadnjih incidentov in koordinaciji njenih aktivnosti so bile zaznane slabosti. Zavedati se moramo, da se vsakodnevno srečujemo s kibernetskimi grožnjami in ranljivostmi informacijsko-komunikacijskih sistemov, ki bi v primeru realizacije lahko imeli težko popravljive posledice za državo in gospodarstvo. V času predsedovanja Svetu EU v drugi polovici leta 2021 smo pred izzivom zagotavljanja razpoložljivosti, dostopnosti in zaupnosti informacijsko-komunikacijskih sistemov, povezanih s predsedovanjem. Kibernetsko varno predsedovanje bo ključno za ugled države. Tudi v ta namen moramo dvigniti raven odpornosti. Zato je nujna čimprejšnja ustrezna umestitev pristojnega nacionalnega organa, ki mora takoj prevzeti proaktivno vlogo na področju informacijsko-kibernetske varnosti.

VI. PRILOGE