PRILOGA 1 (spremni dopis – 1. del):

Ministrstvo za javno upravo RS gp.mju@gov.si
Številka: 007-644/2017-81
Ljubljana, 19. 1. 2018
EVA 2017-3130-0029
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE Gp.gs@gov.si

ZADEVA: Zakon o informacijski varnosti (EVA 2017-3130-0029) – predlog za obravnavo – Novo gradivo št. 2

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 informacijski varnosti (EVA 2017-3130-0029) in ga pošlje v obravnavo in sprejetje Državnemu zboru Republike Slovenije po rednem zakonodajnem postopku.

Mag. Lilijana Kozlovič

GENERALNA SEKRETARKA

Sklep prejmejo:

- Ministrstvo za javno upravo RS,
- Služba Vlade RS za zakonodajo,
- Urad Vlade RS za komuniciranje,
- Generalni sekretariat Vlade RS.

Priloga:

- Zakon o informacijski varnosti

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:

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

3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:

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

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

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

5. Kratek povzetek gradiva:

Ministrstvo za javno upravo (MJU) je pripravilo osnutek predloga Zakona o informacijski varnosti (v nadaljnjem besedilu: ZIV). Z ZIV se sistemsko ureja področje informacijske varnosti v Republiki Sloveniji (v nadaljnjem besedilu: RS) ter se hkrati v nacionalni pravni red prenaša Direktiva 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: Direktiva 2016/1148/ES).

Predlog ZIV ureja ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v RS, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah, zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti in ureja zagotavljanje kibernetske obrambe v RS. Določa minimalne varnostne zahteve in zahteve za priglasitev incidentov za zavezance tega zakona. Prav tako ureja pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa, enotne kontaktne točke, nacionalne skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (v nadaljnjem besedilu: nacionalni CSIRT) in skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij v organih državne uprave (v nadaljnjem besedilu: CSIRT organov državne uprave) na področju zagotavljanja informacijske varnosti in kibernetske obrambe.

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	DA
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
7.a Predstavitev ocene finančnih posledic nad 40.000 EUR: (Samo če izberete DA pod točko 6.a.)		

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	+ 530.000 €	+ 1.020.800 €	+ 1.398.800 €	+ 1.368.800 €
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
Ministrstvo za javno upravo	Projekt informacijska varnost (šifra 3130-17-0009)	PP170089 Razvoj, vzdrževanje in upravljanje informacijske varnosti	530.000 €	/
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:

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

1. vzpostavitve in delovanja Uprave RS za informacijsko varnost (v nadaljnjem besedilu: uprava);
2. zagotovitve pogojev za delovanje CSIRT organov državne uprave na ministrstvu, pristojnem za omrežja in informacijske sisteme organov državne uprave;
3. zagotovitve pogojev za izvajanje nalog drugostopenjskega organa pri reševanju pritožb zoper odločbe, ki jih izda pristojni nacionalni organ po tem zakonu, in za izvajanje nalog strokovne pomoči pri upravljanju pristojnega nacionalnega organa;
4. zagotovitve pogojev za delovanje nacionalnega CSIRT.

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

Ocenjeni stroški vzpostavitve pristojnega nacionalnega organa:

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

Do pričetka delovanja uprave bo njena vzpostavitev potekala na UVTP kot pristojnem nacionalnem organu (PNO). Ocena temelji na projekciji končnega števila novih zaposlitev po letih, in sicer v letu 2018 pet, v letu 2019 devet ter v letih 2020 in 2021 sedemnajst zaposlitev, in pripadajočih stroških ter stroških za investicije v strojno in programsko opremo, ne vključuje pa stroškov nakupa oziroma pridobitve prostorov. Od petih novih zaposlitev leta 2018 sta dve za izvajanje inšpekcijskih in nadzornih funkcij (ena za izvajalce bistvenih storitev in ponudnike digitalnih storitev ter ena za organe državne uprave), tri zaposlitve pa za namene opravljanja preostalih nalog PNO, vključno z administrativno podporo (kadrovsko, finančno, pravno). Potrebna finančna sredstva za UVTP v višini 103.750 eurov za leto 2018 za dodatne pristojnosti in naloge iz tega zakona zagotovi ministrstvo, pristojno za informacijsko varnost (sedaj MJU) s svoje proračunske postavke PP170089 Razvoj, vzdrževanje in upravljanje informacijske varnosti.

[1] UVTP kot pristojni nacionalni organ
[2] Od tu naprej Uprava RS za informacijsko varnost kot pristojni nacionalni organ.

Presoja zagotovitve dodatnih zaposlitev bo izvedena v skladu s 60. členom sprejetega Zakona o izvrševanju proračuna RS za leti 2018 in 2019 ter sprejetimi sklepi Vlade RS o kadrovskih načrtih organov državne uprave.

S pričetkom delovanja uprave 1. 1. 2019 bo nanjo iz UVTP preneseno pet javnih uslužbencev skupaj s kvotami in finančnimi sredstvi zanje. V letu 2019 so predvidene štiri nove zaposlitve, in sicer ena v sekretariatu MJU za podporo delovanju uprave, ena za izvajanje inšpekcijskih in nadzornih funkcij nad izvajalci bistvenih storitev in ponudniki digitalnih storitev ter dve zaposlitvi za namene opravljanja preostalih nalog PNO. V letu 2020 je predvideno še osem novih zaposlitev, in sicer ena za izvajanje inšpekcijskih in nadzornih funkcij nad izvajalci bistvenih storitev in ponudniki digitalnih storitev ter sedem zaposlitev za namene opravljanja preostalih nalog PNO.

V letu 2021, ko niso predvidene nove zaposlitve, bo uprava tako imela sedemnajst uslužbencev, od tega štiri za izvajanje inšpekcijskih in nadzornih funkcij pri zavezancih po ZIV ter trinajst uslužbencev za opravljanja preostalih nalog PNO.

MJU za leta 2019, 2020 in naprej, ko se vzpostavi uprava, priskrbi redno proračunsko postavko v sklopu razreza proračuna na nivoju ministrstva.

Ocenjeni stroški zagotovitve pogojev za delovanje CSIRT organov državne uprave:

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

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

Ocenjeni stroški zagotovitve pogojev za izvajanje nalog drugostopenjskega organa pri reševanju pritožb zoper odločbe, ki jih izda pristojni nacionalni organ po tem zakonu, in za izvajanje nalog

strokovne pomoči pri upravljanju pristojnega nacionalnega organa (organa v sestavi):

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

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

Ocenjeni stroški zagotovitve pogojev za delovanje nacionalnega CSIRT:

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

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

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

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

Predlog zakona nima posledic za druga javna finančna sredstva.

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:
(Samo če izberete NE pod točko 6.a.)
Kratka obrazložitev

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: DA
- Združenju občin Slovenije ZOS: DA
- Združenju mestnih občin Slovenije ZMOS: DA

Predlogi in pripombe združenj so bili upoštevani:

- v celoti,

Bistveni predlogi in pripombe, ki niso bili upoštevani.

9. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	DA

Datum objave: 8. september 2017
V javno obravnavo osnutka predloga ZIV so bile vključene strokovna, zainteresirana in druge javnosti, saj je bilo gradivo osnutka predloga ZIV objavljeno na Državnem portalu Republike Slovenje, e-uprava v rubriki e-demokracija (https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/ predlog-predpisa.html?id=8587) ter spletnih straneh MJU (http://www.mju.gov.si/si/delovna_podrocja/ informacijska_druzba/javne_objave_predlogi/) z rokom za oddajo pripomb do dne 9. oktobra 2017. Hkrati so bili o javni obravnavi osnutka predloga ZIV še posebej obveščeni nekateri deležniki, kot tudi nekateri državni organi in resorji ter združenja oziroma skupnosti lokalne samouprave, in sicer:

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

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

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

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

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

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

- na splošno pripombo ATVP, da ni jasen »obseg« ZIV oziroma ni jasno, na kak manj oziroma bolj širok nabor subjektov s področja »infrastrukture finančnega trga«, za nadzor katerih je pristojna ATVP, se bo ZIV sploh nanašal, pojasnjujemo, da bo to določila vlada najprej z določitvijo seznama bistvenih storitev, nato pa bodo posamezni IBS določeni z odločbo PNO (določeno v 6. členu, ob upoštevanju določb oziroma meril in metodologije iz 7. člena tega predloga zakona);

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

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

- splošne pripombe SOEK glede uporabe zakona pojasnjujemo, da so operaterji v delu, ko nastopajo kot operaterji omrežja oziroma izvajajo javne komunikacijske storitve (skladno z Zakonom o

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

- splošne pripombe ARNES so bile upoštevane;

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

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

- pripomba BS k 2. členu v smislu, da iz določbe osmega odstavka ni mogoče razbrati razloga, zakaj predlagatelj upošteva specialnost področne ureditve glede zahteve po zagotavljanju varnosti omrežij in sistemov ter prijave incidentov, zgolj v zvezi z ureditvijo, ki izhaja iz EU predpisov (neposredno ali zaradi prenosa), ne pa morebiti specialne ureditve, ki je določena z (drugo) nacionalno zakonodajo, ni bila sprejeta iz razloga, ker to ne bi bilo skladno z Direktivo 2016/1148/ES. Vsak zavezanec mora pregledati ali že ustreza zahtevam iz predloga tega zakona (ne glede na kakšni pravni podlagi je sprejel ukrepe). V kolikor oceni, da že izpolnjuje vse obveznosti, ki mu jih nalaga ta predlog zakona (ne glede na kateri podlagi jih je sprejel), mu ni potrebno samo zaradi predloga tega zakona *pro forma* sprejemati nobenih dodatnih ukrepov/dokumentacije. Če pa obveznostim zadosti le delno, potem ukrepe dopolni v delu, kjer ni skladen z ZIV (glej četrti odstavek 12. člena tega zakona);

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

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

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

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

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

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

- splošno pripombo BS k II. Poglavju- Zavezanci, da se v predlogu zakona izrecno določi, da se zahteve v zvezi z varnostjo omrežij in glede poročanja incidentov ne uporabljajo za BS kot zavezanca, nismo upoštevali iz razloga, ker Direktiva 2016/1148/ES izrecno zahteva vključitev področja bančništvo (konkretne zavezance tudi iz področja bančništvo pa bo določil PNO z odločbo skladno s 6. členom na podlagi meril in metodologije iz 7. člena tega predloga zakona);

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

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

- pripomba AVTP k 5. členu je bila upoštevana;

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

- na pripombe ZB k 5. členu, naj bo seznam zavezancev zaupen in ne javno objavljen, odgovarjamo,

da vodenje in vsebino seznamov sedaj določa 25. člena predloga zakona, prav tako drugi odstavek 3. člena predloga zakona določa kateri podatki se obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost (niso vsi podatki *a priori* tajni in poslovna skrivnost);

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

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

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

- pripombe ZČS k 8. členu glede priglasitve so bile delno upoštevane v sklopu 13. člena, njegov prvi odstavek primeroma navaja katere incidente je potrebno priglasiti, katere informacije ter katere kriterije pri določitvi pomembnosti incidenta je potrebno upoštevati;

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

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

hudih), vsakokratni varnostni načrt mora zato vsebovati možnosti za zmanjšanje verjetnosti incidenta oziroma njegovega učinka (kamor spada tudi ohranitev revizijske sledi oziroma »log fileov«);

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

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

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

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

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

- glede pripomb ZB k 9. členu navajamo (sedaj 14. člen tega predloga zakona), da določba ni povezana z obveznostmi IBS, kar bi člane ZB neposredno zadevalo. Gre za PDS. Elementi, ki se upoštevajo, so skladni z Direktivo 2016/1148/ES. Geografsko območje načeloma ni določeno, treba je namreč upoštevati čezmejni vpliv;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- glede pripombe posameznika TV k 20. členu (sedaj 26. člen) naj se strategija pregleduje pogosteje

kot vsakih 5 let, pojasnjujemo, da zakonsko nalaganje obveznosti pregleda le- te ni smotrno, saj mora PNO, v katerega delokrog spada glede na 10. tč. drugega odstavka 27. člena predloga zakona skrb za pripravo in izvajanje strategije, to izvajati po uradni dolžnosti;

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

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

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

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

- splošne pripombe ZSČ k X. Poglavju, naj se dodatno opredelijo nosilci kontrole skladnosti z zakonom pri zavezancih ter opredeli organ, ki bo določil metodologijo ugotavljanja, ter da naj PNO -ju zakonodajalec v 21. členu naloži tudi ustrezno pristojnost oblikovanja metodologije nadzora, ki se izvaja pri zavezancih ali pa naj se vsebinsko opredeli kot dodaten člen, niso bile upoštevane. Pri nadzoru se uporablja Zakon o inšpekcijskem nadzoru- ZIN (inšpektor je pristojen za vse ukrepe po njem), poleg teh pa lahko inšpektor odredi še ukrepe, ki so določeni v predlogu zakona.. V ZIN je po našem mnenju dovolj podrobno opisano ravnanje inšpektorjev, specifike nadzora nad IBS, PDS in državnimi organi pa so opisane v treh ločenih členih predloga zakona, dodatno pa je poseben ukrep določen še v 36. členu predloga zakona;

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

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

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

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

2016/1148/ES;

- na pripombe ICS k 32. členu glede rokov za pričetek delovanja PNO odgovarjamo, da je po naši oceni postavljen rok (sedaj v 41. členu) izvedljiv, v vladnem gradivu so navedeni tudi resursi, ki bodo dani za ta namen. SI CERT bo izvajal naloge nacionalnega CSIRT. Glede pripomb o razmerju PNO in UVTP pojasnjujemo, da v predlogu predviden 41. člen ureja začetek delovanja PNO (predvidoma tako imenovana »Uprava RS za informacijsko varnost«), ki začne z delovanjem dne 1. januarja 2019. S tem dnem od UVTP prevzame naloge, arhive in dokumentacijo, ki se nanašajo na kibernetsko varnost ter javne uslužbence, pravice proračunske porabe, opremo in druge zbirke podatkov oziroma evidence iz prevzetega delovnega področja. Do pričetka delovanja PNO naloge s področja informacijske varnosti opravlja UVTP skladno s Sklepom o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uradni list RS, št. 6/02 in 17/17).

- pripombe ARNES k 33. členu so bile upoštevane.

Potekale so tudi javne predstavitve v osnutku predvidenih rešitev ZIV (kot je bil le-ta dan v javno obravnavo) deležnikom; in sicer:

- dne 14. 9. 2017 v Ljubljani na Posvetu o prepletanju aktualne zakonodaje glede kibernetske varnosti in poročanja o incidentih,
- dne 6.10.2017 na Direktoratu za informacijsko družbo, MJU, predstavnikom SOS,
- dne 8.11.2017 na konferenci Informacijska varnost, na Inštitutu Jožef Štefan, ter sodelovanje na okrogli mizi.

10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	DA
11. Gradivo je uvrščeno v delovni program vlade:	DA

PODPIS PREDLAGATELJA

Boris Koprivnikar

Minister za javno upravo