Gospodarska zbornica Slovenije

Vodstvo
Dimičeva 13, 1504 Ljubljana, 01 5898 413, www.gzs.si, kabinet@gzs.si

REPUBLIKA SLOVENIJA
Urad Vlade Republike Slovenije za informacijsko varnost
Ulica gledališča BTC 2
1000 Ljubljana
gp.uiv@gov.si

Datum: 4. junij 2024

Zadeva: Predlogi in pripombe Gospodarske zbornice Slovenije k osnutku predloga Zakona o informacijski varnosti z dne 15. 5. 2024.

Urad Vlade Republike Slovenije za informacijsko varnost (v nadaljevanju: URSIV oz. predlagatelj) je strokovno, zainteresirano in drugo javnost pozval k posredovanju komentarjev in predlogov k osnutku predloga Zakona o informacijski varnosti (EVA 2023-1544-0005, v nadaljevanju: osnutek predloga zakona), ki je bil dne 15. 5. 2024 objavljen na portalu E-demokracija.

Gospodarska zbornica Slovenije je osnutek predloga zakona obravnavala v okviru zbornic in združenj ter se posvetovala s svojimi člani Sekcije za kibernetsko varnost (SeKV) in Sekcije operaterjev elektronskih komunikacij (SOEK), ki delujeta v okviru Združenja za informatiko in telekomunikacije pri GZS. V nadaljevanju posreduje svoje pripombe in predloge kot sledi.

A. Predlogi in pripombe Sekcije za kibernetsko varnost (SeKV)

Splošne pripombe:

Uvodoma ugotavljamo, da URSIV v pretežni meri ni upošteval predlogov in pripomb, ki jih je v prvem krogu javne obravnave podalo Združenje za informatiko in telekomunikacije pri Gospodarski zbornici Slovenije. Obenem pa se je predlagana ureditev v nekaterih vidikih še zaostrila v primerjavi s prvim osnutkom, zaradi česar podajamo dodatne predloge in pripombe. Zaradi kompleksnosti obravnavane problematike in izražene pomisleke v zvezi s osnutkom predloga zakona predlagamo, da URSIV opravi tudi javni posvet z izmenjavo stališč zainteresirane javnosti, da se skuša doseči čim širši konsenz okoli obravnavanih vprašanj.

Izpostavljamo še nekaj možnosti za izboljšavo osnutka predloga zakona:

1. V osnutku predloga zakona se uporablja več izrazov: kibernetska, informacijska in računalniška varnost. Predlagamo, da se besedilo terminološko uskladi, da se izrazi ne multiplicirajo in uvajajo dodatne nejasnosti.

2. Menimo, da inšpekcija kot sestavni del URSIV-a ni najboljša organizacijska rešitev. Uvedba inšpekcijskih praks, kot jih na primer določata uredbi eIDAS in GDPR, bi bila primernejša rešitev. Vse člene in določbe, ki se nanašajo na inšpekcijski nadzor, je potrebno uskladiti z Zakonom o inšpekcijskim nadzoru. V osnutek predloga zakona naj se doda uvodna določba, da se med inšpekcijskim postopkom ne sme motiti delovanje subjekta, kot je navedeno v Direktivi NIS 2 in kot to za presoje določa tudi ISO 27001.

Podrobni komentarji po členih:

- **K 2. členu osnutka predloga zakona (namen zakona)**

Predlagamo, da se 2. člen osnutka predloga zakona spremeni tako, da se namen zakona še dodatno opredeli in natančneje definira.
Hkrati pozdravljamo odločitev URSIV-a, da v osnutku predloga zakona uredi tudi izvajanje Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (v nadaljevanju: Uredba EU 2019/881).

- **K 1. odst. 3. člena osnutka predloga zakona (področje uporabe zakona)**

Menimo, da so potrebna bolj jasna merila za presojanje ustreznosti oz. sorazmernosti ukrepov za obvladovanje tveganj ter izvajanje ukrepov v praksi.

- **K 5. členu osnutka predloga zakona (pomen izrazov)**

Menimo, da je v 2. točki 5. člena osnutka predloga zakona potrebno poenotiti izraze zato predlagamo, da se beseda »računalniške« zamenja z besedo »informacijske«.

Predlagamo, da se 39. točka 5. člena osnutka predloga zakona spremeni tako, da se glasi: »Preizkušeni revizor pomeni preizkušenega revizorja informacijskih sistemov, ki je pridobil strokovni naziv pri Slovenskem inštitutu za revizijo in je vpisan v njegov register aktivnih preizkušenih revizorjev informacijskih sistemov.«
Predlagamo dodatni premislek glede določbe 39. točke 5. člena, ki določa Slovenski inštitut za revizijo kot edini organ, pri katerem je možno pridobiti strokovni naziv. Uveljavitev te določbe bi lahko vodila v omejevanje konkurence.

Menimo, da glede na vsebino 68. in 69. točke osnutka predloga zakona ni jasno na podlagi katerih zakonskih določb se bo ukrepalo zoper posameznika, ki bo "varovani podatek" razkril nepoklicani osebi. "Varovani podatek" ni ena od izjem od dostopa javnosti do informacij organa, ki so določene v 6. členu Zakona o dostopu do informacij javnega značaja (ZDIJZ). Definicija "varovanega podatka" ustreza opredelitvi tajnega podatka stopnje tajnosti INTERNO, ki se nanaša na javno varnost, kot ga opredeljuje Zakon o tajnih podatkih (ZTP).

- **K 6. členu osnutka predloga zakona (zavezanci)**

Iz določb 2. odstavka 6. člena osnutka predloga zakona ni dovolj razvidno ali gre za javne ali zasebne subjekte, ki imajo vsaj 50 zaposlenih in letni promet ali letno bilančno vsoto vsaj 10 milijonov evrov.

Predlagamo črtanje 5. in 8. točke 2. odstavka 6. člena osnutka predloga zakona. Menimo, da ni opravičljivega razloga, da vsi kriteriji za določitev zavezancev ne bi bili določeni v zakonu in da je dopuščeno Vladi RS, da sama (brez vnaprej zakonsko določenih kriterijev) določi dodatne zavezance. Menimo, da bi bilo takšno blanketno pooblastilo tudi v nasprotju s 120. in 87. členom Ustave RS.

- **K 1. odstavku 7. člena osnutka predloga zakona (samoregistracija in seznam zavezancev)**

Predlagatelj ni z ničemer utemeljil svoje odločitve, da bo vzpostavitev in evidentiranje statusa bistvenih in pomembnih subjektov, razen redkih izjem, temeljilo na samoidentifikaciji in samoregistraciji bistvenih in pomembnih subjektov. Še vedno menimo, da bi bil učinkovitejši in natančnejši sistem registracije zavezancev, ki bi temeljil na podatkih uradnih evidenc.

Primer ureditve vodenja registra zavezancev za informacije javnega značaja v Zakonu o dostopu do informacij javnega značaja (ZDIJZ), kaže, da že imamo hibridni sistem registracije zavezancev, ki namesto na samoregistraciji prvenstveno temelji na obdelavi obstoječih podatkov uradnih evidenc. Upravljavec registra in nosilec postopka evidentiranja zavezancev je AJPES (členi 3.b, 3.c in 3.d ZDIJZ).

- **K 15. člena osnutka predloga zakona (sodelovanje skupin CSIRT z deležniki zasebnega sektorja)**

Menimo, da v 15. členu osnutka predloga zakona ni jasno opredeljena identifikacija skrbnika sistema (kje CSIRT pridobi informacijo o skrbniku sistema).

- **K 19. členu osnutka predloga zakona (upravljanje)**

Predlagamo dopolnitev 19. člena osnutka predloga zakona tako, da se določi, da pristojni nacionalni organ začne izvajati program za usposabljanje odgovornih oseb najkasneje v 4 mesecih po uveljavitvi zakona.

- **K 20. členu osnutka predloga zakona (varnostna dokumentacija bistvenih in pomembnih subjektov)**

Predlagamo črtanje dela besedila v 4. odstavku 20. člena osnutka predloga zakona: »način izvajanja obveznosti iz tega člena. Pri tem vlada upošteva tudi morebitne dokumente ali tehnična priporočila ENISA, Skupine za sodelovanje in dokumente Evropske komisije.«.
Menimo, da bi šlo za nalaganje obveznosti s podzakonskim aktom in za blanketno pooblastilo, ki bi bilo v nasprotju s 120. in 87. členom Ustave RS, ker zakon ne določa dovolj podrobno usmeritev za podzakonsko urejanje.

- **K 21. členu osnutka predloga zakona (ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov)**

Predlagamo, da se v 5. odstavku 21. člena osnutka predloga zakona besedilo »rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih lahko pripravi Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA« nadomesti z besedilom »rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki bodo izvedene v skladu s členom 22(1) Direktive 2022/2555.« Menimo namreč, da je zdajšnji 5. odstavek bistveno manj določen kot člen 21(3) Direktive NIS 2. V členu 21(3) Direktive NIS 2 je razvidno, da se določba nanaša na konkretne ocene tveganj, ki bodo izvedene na podlagi 22. člena Direktive NIS 2 in ne kar splošno. Predlagamo, da se neskladje odpravi.

Kot razumemo je predlagatelj z novim osnutkom predloga zakona upošteval digitalno infrastrukturo, bančno infrastrukturo in infrastrukturo finančnega trga kot subjekte, ki jim ni treba voditi dnevnikov lokalno v Sloveniji. Menimo, da bi bilo koristno razširiti izjemo v 6. odstavku 21. člena osnutka predloga zakona in omeniti tudi "subjekte v storitvah upravljanja IKT in digitalne ponudnike". Te spremembe bi prinesle znatne koristi in bi bile skladne s cilji osnutka predloga zakona. Z omogočanjem shranjevanja dnevniških zapisov v EU bi zagotovili, da so podatki shranjeni varno in skladno, hkrati pa bi zagotovili večjo prožnost za subjekte v storitvah upravljanja IKT in ponudnike digitalnih storitev.

Predlagamo črtanje (ali vsaj spremembo) 9. odstavka 21. člena osnutka predloga zakona. Nista določena način in rok ugotavljanja ali imajo informacijsko-komunikacijske rešitve aktivno izkoriščane ranljivosti, kdo to ugotavlja in po kakšnem postopku. Prav tako nista določena rok in način v katerem je potrebno izvesti prilagoditev itd. Vprašanje morebitnih ranljivosti je že naslovljeno z drugimi določbami, npr. glede priprave dokumentacije, obvladovanja tveganj, varnostnih ukrepov, kar se nanaša tudi na morebitne ranljivost. Postavlja se vprašanje, zakaj bi

moral za ranljivosti veljati poseben neizdelan sistem s celo vrsto nedorečenih vprašanj in pravnih praznin. Menimo, da je trenutna določba povsem neizdelana in vsebuje pravno praznino, ter da je to tveganje že naslovljeno s preostalimi določbami.

Predlagamo, da se 11. odstavek 21. člena osnutka predloga zakona črta.
Menimo, da bi bilo tako široko blanketno pooblastilo verjetno v nasprotju z Ustavo RS in problematično v praksi. Skladno z drugim odstavkom 120. člena Ustave RS upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov (legalitetno načelo), kar vključuje tudi zahtevo po vsebinski vezanosti upravnih organov na ustavo in zakon, ki zagotavlja, da se posamezniki in pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali. Skladno s 87. členom Ustave RS pa lahko pravice in obveznosti državljanov ter drugih oseb državni zbor določa le z zakonom, kar predstavlja tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon. Predlagatelj je urejanje materije iz 11. odstavka 21. člena v celoti prepustil podzakonskemu predpisu vlade, kar je v nasprotju z ustavnim načelom legalitete, še posebej, ker lahko omejitve glede dobavnih verig posegajo na trg (torej tudi na prosto nastopanje dobaviteljev na trgu) in s tem omejitev ali določitev načina uresničevanja svobodne gospodarske pobude (74. člen Ustave RS). Navedene problematike po vsebini ne reši dikcija, da naj bi vlada določala zgolj »način izvajanja obveznosti« in »varnostne ukrepe«, saj je vsebina 21. člena zelo splošna (na nivoju smernic, ki splošno govorijo o obveznosti sprejeti ustrezne ukrepe) in nekonkretizirana. Predpisovanje načina izvajanja obveznosti sprejeti ustrezne ukrepe, pa bi bilo dejansko originarno predpisovanje ukrepov in bi obenem predstavljalo določitev načina uresničevanja svobodne gospodarske pobude, kar bi še vedno morala biti zakonska materija. Glede na odprtost in splošnost 21. člena preprosto ni mogoče šteti, da bi vlada s podzakonskim predpisom sploh lahko podrobneje urejala zakonsko materijo in pri tem sledila namenu in ciljem zakona. Dodatno v zvezi z 10. točko 2. odstavka 21. člena to pomeni, da bi vlada lahko (brez zakonskih kriterijev) urejala tudi tveganja, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev ter v zvezi s 5. odstavkom 21. člena »ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev«. Navedeno nakazuje na možnost izključevanja posameznih dobaviteljev iz naslova naslavljanja specifičnih ranljivosti vezanih na določenega dobavitelja, v zvezi s čimer se odpirajo številni pomisleki. Vsekakor vlada ne bi smela imeti pristojnosti omejevanja trga dobave opreme in storitev, ne da bi bili v zakonu podrobno opredeljeni kriteriji (kot jih na primer opredeljuje 117. člen ZEKom-2).

- **K 22. členu osnutka predloga zakona (obveza posredovanja podatkov in informacij)**

Menimo, da je 22. člen osnutka predloga zakona presplošen in presega vsebino Direktive NIS 2. Predlagamo, da se inšpekcijske/nadzorstvene pristojnosti omejijo na pristojnosti, ki jih predvideva Direktiva NIS 2 (ki so že rezultat tehtanja med drugim tudi z vidika sorazmernosti in procesnih jamstev) in za katere menimo, da so že široke. Navedeno velja splošno tudi za preostale določbe v osnutku predloga zakona glede nadzora in inšpekcijskih pristojnosti.

- **K 23. členu osnutka predloga zakona (certificiranje)**

Naša bistvena pripomba se nanaša na določbo v 1. odstavku, ki definira pojem certifikacije in na 9. odstavek, v katerem je definirana Izjava EU o skladnosti. Predlagamo, da se v zvezi z Izjavo EU o skladnosti upoštevajo določila 53. člena Uredbe (EU) 2019/881 (samoocenjevanje skladnosti) in se jasno razmeji med »Evropskim certifikatom kibernetske varnosti« in »Izjavo EU o skladnosti«, pri čemer se vsak od njiju nanaša na katero koli raven zanesljivosti, določeno v evropski certifikacijski shemi za kibernetsko varnost, v okviru katere se evropski certifikat kibernetske varnosti ali izjava EU o skladnosti izda. V 15. odstavku je obravnavana zgolj izdaja in

podpis Izjave EU o skladnosti, ne pa tudi predložitev nacionalnemu certifikacijskemu organu za kibernetsko varnost in agenciji ENISA.

Slovenija je dolžna do 27. 2. 2025 določiti nacionalni certifikacijski organ za kibernetsko varnost (3. odstavek) in organ(e) za ugotavljanje skladnosti, ki so v tem zakonu določeni na način opredeljen v 4. in 5. odstavku.

Kadar se odkrijejo morebitne neskladnosti, ki vplivajo na certificirani proizvod IKT, storitev IKT in postopke IKT, je pomembno zagotoviti sorazmeren odziv in ne le odvzem certifikata, ampak tudi začasni preklic (8. odstavek). Tudi sicer naj bo postopek skladen s členi Uredbe (EU) 2019/881 in izvedbenimi uredbami za posamezno evropsko certifikacijsko shemo za področje izdajanje, podaljšanja in odvzema.

V 10. odstavku predlagamo uporabo veznika in »Fizične **in** pravne osebe imajo pravico …«

Predlagamo črtanje od 6. do vključno 16. odstavka 23. člena osnutka predloga zakona. Menimo, da s preuranjeno regulacijo odprtih vprašanj Republika Slovenija tvega neskladnost s prizadevanji za harmonizacijo tega področja na ravni EU.

Menimo, da je celoten 23. člen nejasen tako redakcijsko kot tudi terminološko in vsebinsko. Niso jasno razmejeni nacionalno izdani certifikati, certifikati izdani na ravni EU ter certifikati izdani s strani drugih držav članic. 23. člen osnutka predloga zakona omenja možnost odvzema evropskih certifikatov za kibernetsko varnost brez jasne navedbe, da so s tem mišljeni zgolj certifikati izdani v Sloveniji po zakonu o informacijski varnosti, ne pa tudi morebiti drugi evropski certifikati.

Menimo, da je potrebno oceniti, ali ima URSIV, ki je v na podlagi 9. člena osnutka predloga zakona določen kot pristojni nacionalni organ, kapacitete (zadostno število zaposlenih), strokovnost ter izkušnje za izvajanje vseh nalog, ki mu jih podeljuje osnutek predloga zakona. URSIV ima relativno malo zaposlenih in še ti delujejo na 6 različnih oddelkih, ustreznost strokovnega znanja in izkušenj pa je zahtevana že po sami Uredbi EU 2019/881, ki v tretjem odstavku 59. člena določa, da se z medsebojnim strokovnim pregledom ocenjuje, ali ima osebje organov, ki izdajajo certifikate za „visoko“ raven zanesljivosti v skladu s členom 56(6), ustrezno strokovno znanje in izkušnje.

Upoštevaje, da je bila ravnokar šele sprejeta prva evropska certifikacijska shema (tako imenovana »EUCC« shema), in da sta dve shemi še vedno v pripravi (»EUCS« shema in »EU5G« shema, katerih priprava bo zagotovo trajala štiri do pet let), se zdijo predlagani 6., 7. in 8. odstavek preuranjeni in nesmiselni. Primerjalno gledano večina drugih evropskih držav še ni začela sprejemati zakonodaje, s katero bi spreminjala ureditev glede evropskih certifikacijskih shem. V skladu z informacijami, dostopnimi na spletni strani ENISE (https://www.enisa.europa.eu/topics/certification/eu-cybersecurity-certification-faq), bo potrebno najprej še sprejeti izvedbeni akt na ravni EU, ki ga bodo morale potrditi vse države članice. Šele po tem, ko bo navedeni akt sprejet, bodo imele države članice čas, da bodo pripravile vse potrebno za delovanje sheme in izdajanje potrdil. Preden bodo izpolnjeni vsi opisani koraki, bo trajalo še več let, zato ni smiselno sprejemati določb, kot so navedene v 6. in nadaljnjih odstavkih 23. člena, saj se utegnejo izkazati za nasprotne skupnim prizadevanjem harmonizacije certifikacije na ravni EU. Ne zdi se primerno, da bi Slovenija kot majhna in izvozno naravnana država (ki se v veliki meri zanaša na odprt enotni trg) z relativno omejenimi (tehničnimi, strokovnimi in kadrovskimi) zmožnostmi za vzpostavitev lastne certifikacijske sheme, prispevala k drobitvi evropskega trga in vzpostavitvi svojih specifičnih omejitev na trgu opreme in storitev. Navedeno toliko bolj drži upoštevajoč člen 57 Uredbe EU 2019/881, ki

določa, da bodo nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za proizvode IKT, storitve IKT in postopke IKT, ki so zajeti v evropski certifikacijski shemi za kibernetsko varnost, prenehale učinkovati z datumom, določenim v izvedbenem aktu, sprejetem na podlagi člena 49(7).

Menimo, da je v 10. odstavku sklic na »izjave EU o skladnosti« preširoko definiran, saj je možno govoriti le o izjavah po CSA (vezanih na kibernetsko varnost) in ne vseh morebitnih izjavah o skladnosti.

12. odstavek 23. člena predvideva pravno sredstvo pred upravnim sodiščem. Menimo, da so tovrstna pravna sredstva zelo omejena in de facto neustrezna (tudi z vidika ustavno varovane pravice do pravnega sredstva oziroma sodnega varstva). Upravno sodišče je v svojih odločitvah večkrat zavzelo stališča glede omejenega sodnega nadzora v upravnem sporu in je omejilo obseg svoje sodne presoje. Zdi se malo verjetno, da bi sodišče interveniralo v primeru odločitve, ki je napačna z dejanskega (tehničnega) vidika vendar brez postopkovnih napak (primeroma: sklep Upravnega sodišča RS I U 559/2014 z dne 15. 10. 2014: »tako je obseg sodne kontrole omejen na presojo pravilnosti postopka in uporabe materialnega prava« in sodba Upravnega sodišča RS I U 1693/2013 z dne 2.4.2014: »po mnenju sodišča tudi v to sodišče ne more posegati in se zaradi tega do teh tožbenih navedb ne more opredeliti, ker ne gre za pravno, ampak strokovno tehnično vprašanje.«).
Zdi se primerneje, da bi bil postopek dvostopenjski, zoper odločbe pa bi bilo dovoljeno tudi pravno sredstvo pritožbe na organ s strokovnimi kompetencami, ki bi odločitev lahko preveril tudi s strokovno-tehničnega vidika (in ne samo z vidika vsebinskega preizkusa omejeno pravno sredstvo tožbe v upravnem sporu).

Menimo, da je v 13. odstavku 23. člena sklicevanje na postopek »priznanja evropskega certifikata kibernetske varnosti« neustrezno, saj bi moralo biti zapisano, da evropski certifikati kibernetske varnosti veljajo avtomatično tudi v Republiki Sloveniji.

Postopek, v katerem se predvideva »priznanje« evropskega certifikata kibernetske varnosti s strani slovenskih sodišč je povsem v nasprotju z evropsko zakonodajo. V skladu s členom 49(7) Uredbe EU 2019/881 namreč lahko Komisija na podlagi predloge za shemo, ki jo pripravi agencija ENISA, sprejme izvedbene akte, ki določajo evropsko certifikacijsko shemo za kibernetsko varnost za proizvode IKT, storitve IKT in postopke IKT, ki izpolnjujejo zahteve iz členov 51, 52 in 54. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 66(2). Nadalje člen 56 določa, da se za proizvode IKT, storitve IKT in postopke IKT, ki so bili certificirani na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49, domneva, da so skladni z zahtevami take sheme. Certificiranje za kibernetsko varnost je prostovoljno, razen če je v pravu Unije ali države članice določeno drugače. Na podlagi navedenega je jasno, da kakršno koli potrjevanje evropskega certifikata kibernetske varnosti, ki ga je izdal za to pristojni organ druge države članice Evropske unije in ga imajo v lasti zadevne fizične ali pravne osebe, ni skladno z evropsko zakonodajo.

Menimo, da 14. odstavek 23. člena osnutka predloga zakona vsebuje nejasno določbo, saj krog zavezancev, ki jih zavezuje obveznost iz dotičnega odstavka, ni jasno določen, ravno tako ni jasne reference, na katero konkretno odločitev Evropske komisije naj bi bila vezana ta določba ter ni jasno v zvezi s čem naj bi bile določene takšne »kategorije«. Posledično v primeru sprejema delegiranih aktov Evropske komisije ne bo moglo biti jasno, ali gre za akt v smislu 14. odstavka ali ne in naslovniki ne bodo vedeli, kaj je njihova obveznost v skladu s tem odstavkom. Ko oziroma če bo sprejet delegirani akt Evropske komisije, bo šele jasno, kaj je njegova vsebina in šele tedaj ga bo mogoče ustrezno implementirati, kakršnokoli vnaprejšnje naslavljanje tega

vprašanja pa je preuranjeno in neustrezno.

Za določbo 15. odstavku 23. člena osnutka predloga zakona menimo, da presega vsebino Direktive NIS 2. Predlagamo, da se pristojnosti v osnutka predloga zakona omejijo na pristojnosti, ki jih predvideva Direktiva NIS 2, in ki so že rezultat tehtanja med drugim tudi z vidika sorazmernosti in procesnih jamstev in so že relativno široke.

Po določbah 16. odstavka osnutka predloga zakona lahko vlada določenim kategorijam bistvenih subjektov predpiše obvezno uporabo certificiranih proizvodov IKT, storitev IKT ali postopkov IKT. Ni videti opravičljivega razloga, da vsi kriteriji za določitev zavezancev ne bi bili določeni v zakonu in da je dopuščeno vladi, da sama, brez vnaprej zakonsko določenih kriterijev, določi dodatne zavezance (5. točka in 8. točka drugega odstavka). Zato predlagamo, da se 16. odstavek črta, takšno blanketno pooblastilo pa bi bilo tudi v nasprotju s 120. in 87. členom Ustave RS.

- **K 24. členu osnutka predloga zakona (standardizacija)**

Menimo, da bi vlada morala z uredbo (kot pri obstoječem Zakonu o informacijski varnosti (ZInfV) z Uredbo o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev) določiti SUVI in SUNP dokumentacijo, poleg objav na spletni strani pa pošiljati tudi obvestila na spletne naslove zavezancev, vključno z opozorili na relevantne dokumente ENISA. Imamo že dobro prakso, ki bi jo lahko ohranili, in sicer 12. člen obstoječega Zakona o informacijski varnosti (ZInfV).

- **K 26. člena osnutka predloga zakona (postopek priglasitve pomembnih incidentov)**

Postopek priglasitve t.i. pomembnih incidentov je določen zelo natančno in strokovno korektno. Kakšen pa bo postopek priglasitve (časovni roki, vsebina priglasitve, ocena vplivov idr) incidentov, ki ne bodo izpolnjevali meril za razvrstitev med "pomembne"?
Po določbah člena 23(3) Direktive NIS 2 oziroma 1. odstavka 25. člena predmetnega osnutka predloga zakona je incident pomemben, če:
-je zadevnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube;
-je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.
Menimo, da je potrebna določitev postopka za priglasitev vseh incidentov in tudi način poročanja o incidentu, o katerem je potrebno obvestiti več pristojnih državnih organov, npr. poleg URSIV še Informacijskega pooblaščenca, AKOS, Urad Vlade RS za varovanje tajnih podatkov, Inšpektorat za informacijsko družbo ipd.

- **K 27. členu osnutka predloga zakona (pristojnost in teritorialnost)**

Pozdravljamo spremembo v smislu približevanja vsebini Direktive NIS 2, pa vendar vseeno predlagamo, da se teritorialna pristojnost v izogib dvomom bolj jasno zapiše, ne samo glede pristojnosti nacionalnega organa in CSIRT, temveč tudi glede uporabe preostalih določb zakona, da se le-te uporabljajo samo za zavezance iz Republike Slovenije (z relevantnimi izjemami). Če subjekti ne sodijo v pristojnost Republike Slovenije po Direktivi NIS 2, potem tudi ne morejo biti podvrženi slovenski zakonodaji o informacijski varnosti.
Teritorialna pristojnost je urejena zgolj parcialno v 27. členu, in sicer vezano na pristojnost skupine CSIRT in pristojnost URSIV, ni pa teritorialna pristojnost dovolj splošno zapisana v skladu z NIS 2. Menimo torej, da je 27. člen osnutka predloga zakona potrebno uskladiti s členom 26(1) Direktive NIS 2 tako, da se (v 3. člen ali na drugem ustreznem mestu) doda teritorialna pristojnost (za vso materijo), kakor jo določa Direktiva NIS 2.
Povsem nesorazmerna bi bila obveznost, da bi preostale določbe zakona (v nasprotju z Direktivo NIS 2) imele univerzalno veljavnost (vključno z obveznostjo samoregistracije po 7. členu) in bodo

veljale za vse subjekte po celem svetu, tudi takšne, ki nimajo povezave z Republiko Slovenijo (in ne izvajajo storitev v RS in v njej nimajo sedeža). Navedeno predstavlja tudi tveganje za multinacionalke in za pravne osebe s sedežem v Republiki Sloveniji, da bi tudi vse njihove povezane osebe (npr. sestrske družbe in nadrejene družbe) morale izvajati samoregistracijo v Republiki Sloveniji v nasprotju z namenom Direktive NIS 2. Navedeno tudi ruši koncept Direktive NIS 2 glede registracije po posameznih državah, saj bi se bile družbe zavezane samoregistrirati tudi v Republiki Sloveniji (poleg registracije v relevantni pristojni državi EU).

- **K 32. členu osnutka predloga zakona (vrednotenje incidenta in ukrepanje)**

Predlagamo črtanje od 4. do 8 odstavka 32. člena osnutka predloga zakona, saj menimo, da niso v skladu z Direktivo NIS 2, določajo preširoka pooblastila ter so tudi v nasprotju z načelom jasnosti in določnosti predpisov (kot elementa načela pravne države iz 2. člena Ustave RS).
Takšne pristojnosti so preširoke in nedefinirane ter se z njimi osnutek predloga zakona oddaljuje od določb Direktive NIS 2. Zato predlagamo, da se takšne izrecne pristojnosti črtajo. Tako široko blanketno pooblastilo (da se lahko odredijo kakršnikoli ukrepi) je verjetno v nasprotju z Ustavo RS in problematično v praksi. Skladno z drugim odstavkom 120. člena Ustave RS upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov (legalitetno načelo), kar vključuje tudi zahtevo po vsebinski vezanosti upravnih organov na ustavo in zakon, ki zagotavlja, da se posamezniki in pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali. Skladno s 87. členom Ustave RS pa lahko pravice in obveznosti državljanov ter drugih oseb državni zbor določa le z zakonom, kar predstavlja tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon. Predlagatelj je nalaganje obveznosti v celoti prepustil URSIV, kar je v nasprotju z ustavnim načelom legalitete, omejitve pa lahko posegajo tudi na trg (torej tudi na prosto nastopanje dobaviteljev na trgu) in gre s tem tudi za omejitev oziroma določitev načina uresničevanja svobodne gospodarske pobude (74. člen Ustave RS).

- **K 33. členu osnutka predloga zakona (ocena ogroženosti)**

Predlagamo črtanje od 7. do 10. odstavka 33. člena osnutka predloga zakona.
Za obrazložitve se sklicujemo na pripombe k 32. členu osnutka predloga zakona.

- **K 41. členu osnutka predloga zakona (splošne določbe)**

Menimo, da je 41. člen osnutka predloga zakona presplošen in presega vsebino Direktive NIS 2. Predlagamo, da se inšpekcijske/nadzorstvene pristojnosti omejijo na pristojnosti, ki jih predvideva Direktiva NIS 2 (ki so že rezultat tehtanja med drugim tudi z vidika sorazmernosti in procesnih jamstev) in so že relativno široke. V nasprotnem, ko gre za dodatno širjenje pristojnosti, verjetno ne bo podana sorazmernost. Navedeno velja za vse preostale določbe glede nadzora in inšpekcijskih pristojnosti.

- **K 42. členu osnutka predloga zakona (nadzor bistvenih subjektov)**

Menimo, da dodatne pravice inšpektorja določene v 42. členu osnutka predloga zakona niso jasne. Ciljno usmerjene revizije skladnosti iz 2. točke prvega odstavka 42. člena osnutka predloga zakona temeljijo na ocenah tveganj, ki jih izvedejo pristojni nacionalni organi ali bistveni subjekt, ki je predmet presoje, ali na drugih razpoložljivih informacijah o tveganju. Poročilo o izvedeni ciljno usmerjeni reviziji varnosti se da na voljo inšpektorju.

Menimo, da je potrebno vse člene in določbe, ki se nanašajo na inšpekcijski nadzor, uskladiti z Zakonom o inšpekcijskim nadzoru.

Za dodatne obrazložitve se sklicujemo na pripombe k 41. členu osnutka predloga zakona (splošne določbe).

- **K 43. členu osnutka predloga zakona (nadzor pomembnih subjektov)**

Predlagamo črtanje 3. točke 2. odstavka 43. člena osnutka predloga zakona.
Zastavlja se vprašanje ali je določba izvedljiva v okviru nadzora? Varnostni pregled je najsplošnejši izraz, ki označuje proces iskanja varnostnih pomanjkljivosti v sistemih, procesih in ljudeh z dovoljenjem in v dogovoru z lastnikom sredstev z namenom izboljšanja varnosti. Ali pomeni tudi pregled ranljivosti in izvedbo vdornega testiranja?

Za dodatne obrazložitve se sklicujemo na pripombe k 41. in 42. členu osnutka predloga zakona.

- **K 53. členu (prekrški bistvenih subjektov) in 54. členu osnutka predloga zakona (prekrški pomembnih subjektov)**

Menimo, da so globe določene v 53. in 54. členu osnutka predloga zakona previsoke in nesorazmerne. Predlagamo, da se možnost izreka globe v višini 2% prometa rezervira za primere, ki jih predvideva Direktiva NIS 2, in da se takšna izjemno huda sankcija ne širi preko okvirov, določenih v Direktivi NIS 2. Glede na to, da Direktiva NIS 2 predvideva zgolj globo za kršitev člena 21 NIS 2 (ukrepi za obvladovanje tveganj za kibernetsko varnost) in člena 23 NIS 2 (obveznosti poročanja o incidentih), predlagamo, da se tudi osnutek predloga zakona omeji na navedeni dve situaciji.
Vsekakor se zdi primerneje, da se najnižja globa ne bi določala, ali da bi bila najnižja globa določena zgolj v nominalnem znesku (ne v odstotku od prometa, saj so globe določene v odstotku od prometa primerjalno rezervirane za najtežje kršitve). Primerjalno-pravno je bilo prvo področje, kjer so se uveljavile kazni v odstotku od prometa na področju konkurenčnega prava in le-to določa zgolj najvišjo sankcijo (npr. 85. člen Zakona o preprečevanju omejevanja konkurence (ZPOmK-2) do deset odstotkov letnega prometa), ne pa minimalnega zneska, kar omogoča širše polje diskrecije ob izreku sankcije.
Drugačna ureditev ne bi zadostila kriteriju sorazmernosti in bi bila potencialno protiustavna. Osnutek predloga zakona predvideva globo v odstotku od prometa tudi za manj hude kršitve, kar pa ne more biti v skladu s kriterijem sorazmernosti in je posledično potencialno neustavno. Na predlagatelju je obveznost, da bi moral pojasniti in dokazati sorazmernost predlagane globe s kršitvami, česar pa ne bo mogel, ker je že Direktiva NIS 2 posledica tehtanja sorazmernosti med temeljnimi pravicami, rezultat tega tehtanja pa je presoja, da je globa v odvisnosti od prometa (omejena na 2% prometa) primerna in sorazmerna zgolj za kršitvi, ki ju predvideva NIS 2.

- **K 62. členu osnutka predloga zakona (spremembe in dopolnitve Zakona o elektronskih komunikacijah)**

Predlagamo, da se predlogom zakona ne posega v Zakona o elektronskih komunikacijah (ZEKom-2).
Menimo, da ni razloga za predlagane spremembe. Sprememba 115. člena Zakona o elektronskih komunikacijah, ki se sklicuje na obveznosti po zakonu, ki ureja informacijsko varnost, bi morebitne kršitve ZInfV-1 kvalificirala istočasno tudi kot kršitve ZEKom-2, kar pa je nepotrebno podvajanje. Menimo, da bi sprememba 115. člena Zakona o elektronskih komunikacijah, ki predvideva, da lahko agencija izda splošni akt, s katerim predpiše posebne tehnične usmeritve ter tehnične in organizacijske ukrepe, pri čemer upošteva tudi dokumente ali tehnična priporočila ENISA ter smernice Evropske komisije, in da pri sprejemu splošnega akta agencija sodeluje z organom, pristojnim za informacijsko varnost, po vsej verjetnosti bila v nasprotju z Ustavo RS (blanketna norma, ki ne daje zadosti določnih usmeritev za podzakonsko urejanje).

Skladno z drugim odstavkom 120. člena Ustave RS upravni organi opravljajo svoje delo

samostojno v okviru in na podlagi ustave in zakonov (legalitetno načelo), kar vključuje tudi zahtevo po vsebinski vezanosti upravnih organov na ustavo in zakon, ki zagotavlja, da se posamezniki in pravne osebe z bistvenimi elementi svojega pravnega položaja lahko seznanijo že iz zakona in da lahko zaupajo, da podzakonski predpisi ne bodo posegali v te bistvene elemente, posamični akti državnih organov pa bodo ta bistvena upravičenja zagotavljali oziroma tudi varovali. Skladno s 87. členom Ustave RS pa lahko pravice in obveznosti državljanov ter drugih oseb državni zbor določa le z zakonom, kar predstavlja tudi ustavno omejitev, da lahko originarno ureja pravice in obveznosti posameznikov in pravnih oseb le zakon. Predlagatelj je urejanje materije iz 115. člena v celoti prepustil podzakonskemu predpisu AKOS, kar je v nasprotju z ustavnim načelom legalitete, še posebej ker lahko tak splošni akt posega tudi na trg (torej tudi na prosto nastopanje dobaviteljev na trgu) in s tem omejitev ali določitev načina uresničevanja svobodne gospodarske pobude (74. člen Ustave RS). Vsebina 115. člena je tako presplošna in nekonkretizirana.

Sprememba 298. člena Zakona o elektronskih komunikacijah predvideva novo globo do pet odstotkov letnega prometa, ustvarjenega na trgu javnih komunikacijskih omrežij oziroma javnih komunikacijskih storitev v predhodnem poslovnem letu, če se ne izvede odločbe vlade iz prvega odstavka 117. člena. Navedeno predstavlja povsem nesorazmerno globo v nasprotju z načelom sorazmernosti, ki dejansko (še dodatno zaradi odsotnosti možnosti pritožbe in nesuspenzivnosti pravnega sredstva, torej upravnega spora zoper izdano odločbo) izpodbija pravico do sodnega varstva. Operater se bo tako tudi v primeru nezakonite odločbe, pod bremenom grožnje globe do pet odstotkov letnega prometa, prisiljen podrediti odločbi, tudi če je nezakonita in se z njo ne strinja, tudi za čas pred pravnomočnostjo take odločbe dokler je v teku morebitno pravno sredstvo zoper odločbo. Takšen ukrep je nesorazmeren. Takšen predlog bi tudi zahteval vnovično priglasitev po mehanizmu TRIS, saj bi šlo za spremembo (bolj restriktiven poseg) v primerjavi z že priglašenim besedilom ZEKom-2 v okviru TRIS mehanizma.

- **K PRILOGI II - DRUGI KRITIČNI SEKTORJI**

Direktiva NIS 2 ne določa obveznosti za raziskovalne ustanove, vendar peti odstavek 2. člena NIS 2 dopušča, da lahko države članice določijo, da so zavezanci tudi ustanove, ki izvajajo kritične raziskovalne dejavnosti. Glede na to, da pravo EU ne zahteva, da se mora zakon o informacijski varnosti uporabljati tudi za te ustanove, bi bilo v zvezi z navedeno razširitvijo uporabe NIS 2 potrebno izvesti tudi presojo posledic za gospodarstvo in upoštevati načelo sorazmernosti. Ne zdi se skladno z načelom enakosti in načelom sorazmernosti, da bi se zakon o informacijski varnosti uporabljal za vse raziskovalne ustanove, temveč bi bilo navedeno (če bo predlagatelj utemeljil in dokazal, zakaj bi bila takšna ureditev primerna, nujna in sorazmerna v ožjem pomenu) omejiti na raziskovalne ustanove, ki izvajajo »kritične raziskovalne dejavnosti«. Npr. če je mogoče videti utemeljeni interes zakaj se pri raziskovalni ustanovi, ki se ukvarja z jedrskimi raziskavami ali na primer upravlja jedrski reaktor, zahteva višja stopnja kibernetske varnosti, takšne situacije ni mogoče enačiti z raziskovalnimi ustanovami, ki niso varnostno občutljive oziroma »kritične« (npr. sociološke raziskave). Predlagamo ustrezno zamejitev skladno z Direktivo NIS 2.

B. Predlogi in pripombe Sekcije operaterjev elektronskih komunikacij (SOEK)

Splošne pripombe:

1. Obrazložitev posamičnih členov

Obrazložitev k vsakem posamičnem členu ne dodaja popolnoma nobenega pojasnila, obrazložitev je vsebinsko prazna in zgolj prepiše besedilo samega člena, kar je nesprejemljivo in najverjetneje v nomotehničnem smislu prepovedano (gl. navodila za izvajanje Poslovnika VRS št. 1000400-5/2014/23 z dne 20.6.2027, spremenjen 21.11.2019 – v prilogi 3 je določena minimalna vsebina obrazložitve predloga predpisa). Ker je obrazložitev vitalnega pomena za razumevanje tega kompleksnega prepisa predlagamo, da se obrazložitve k členom ustrezno dopolnijo in pojasni smisel ter namen posamične norme.

2. Obligatornost izdaje podzakonskih predpisov

Na več mestih osnutek predloga zakona preveč splošno in ohlapno opredeljuje obveznosti subjektov, zato predlagamo, da se te obveznosti zaradi načela transparentnosti, jasnosti in predvsem pravne varnosti, natančneje opredelijo. Subjekti zavezanci stremijo k temu, da so jim njihove obveznosti jasne in poznane vnaprej, ker se bojo le tako lahko prilagodili in zakon izvajali na način, kot je predviden.

3. Prehodne določbe

V prehodnih določbah se večkrat omeni, da veljavni podzakonski predpisi veljajo do izdaje novih. Predlagamo, da se natančno navede kateri novi podzakonski predpisi bodo izdani na podlagi predmetnega zakona, saj je to nekoliko težko ugotoviti.

Podrobni komentarji po členih:

- **K 5. odst. 4. člena osnutka predloga zakona (obdelava podatkov in informacij)**

Po določbi 5. odstavka 4. člena osnutka predloga zakona, ki je bil pa sicer delno spremenjen, se podatki in informacije, ki se obdelujejo po tem zakonu in so vitalni za nacionalni interes, ne smejo iznašati izven Republike Slovenije. To je v spremenjenem odstavku omenjeno dvakrat. Iz popravka člena izhaja, da velja prepoved za organe državne uprave, a je treba zaradi pomembnosti tega določila, še enkrat preučiti kaj je želel predlagatelj predpisati in to jasneje zapisati.

- **K 25. (obveznost priglašanja in obveščanja), 26. (postopek priglasitve pomembnih incidentov) členu osnutka predloga zakona ter spremembi Zakona o elektronskih komunikacijah ter vzpostavljanju informatiziranega sistema za poročanje**

Skladno z zakonom o elektronskih komunikacijah Agencija za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju: AKOS) v zadnjih nekaj mesecih vzpostavlja informatiziran sistem, med drugim tudi za poročanje incidentov, čeprav osnutek predloga zakona predvideva, da se bodo ti incidenti prijavljali URSIV in ne več AKOS-u. AKOS se je že pozvalo, da z vzpostavitvijo sistema počaka do uskladitve poročanja med organoma (URSIV in AKOS), verjetno pa najkasneje do sprejema predmetnega zakona.

Poročanje incidentov, kot je predvideno z osnutkom predloga zakona, je izredno neopredeljeno, zato predlagamo, da se predvidi izdaja podzakonskega predpisa, v katerem naj se (po vzoru ureditve ZEKom-2) definirata postopek poročanja ter nabor podatkov za poročanje oziroma vsaj predvidi obrazec, iz katerega bi izhajali podatki, ki jih morajo subjekti zbirati in poročati naslovnemu organu/CSIRT/ostalim. Nasprotujemo nedefiniranosti saj ekipe zavezancev niso dimenzionirane na način, da se nenehno prilagajajo spremembam pri poročanju (ne NOC, SOC

ali IT), niti da se zahtevajo različni podatki. Predlagamo, da predlagatelj preuči druge države članice EU, ki so Direktivo NIS 2 že implementirale in preveri na kakšen način posamične države urejajo poročanje incidentov.
Predlagamo, da se kar v največji možni meri izogne poročanju incidentov preko elektronske pošte ter apeliramo, da se takoj preide na avtomatiziran sistem. Za to ne obstojijo nobeni zadržki, posebej spričo dejstva, da je ta sistem za povsem primerljive potrebe v državi že vzpostavljen.
Ker AKOS vzpostavlja informatiziran sistem za poročanje, menimo, da bi bilo smiselno, da se ta sistem poročanja uporabi tudi za potrebe poročanja po tem osnutku predloga zakona. Tako bi najhitreje prešli na avtomatizirano poročanje. V osnutku predloga zakona se lahko predvidi prilagoditveni rok, ki je lahko kratek, saj je AKOS sistem poročanja že razvil. Kategorije poročanih podatkov je potrebno prilagoditi in, kot že omenjeno, opredeliti katere podatke o incidentu so subjekti dolžni poročati.
Upoštevaje, da sistem obveščanja za operaterje elektronskih komunikacij ni nov, predlagamo, da se ureditev, ki je v veljavi že danes ter je opredeljena v ZEKom-2, ustrezno prilagodi zahtevam predmetnega zakona. Tako bi se v čim večji meri ognili težavam pri implementaciji.
Predlagamo tudi, da se:
-v kolikor priglasitveni organ nima dežurne službe, rok za obveščanje opredeli »naslednji delovni dan«;
-poenostavijo obveščanja, ker osnutek predloga zakona brez razlage zahteva ogromno poročanja, pri čemer so v primeru incidenta, prizadevanja subjektov usmerjena v odpravo incidenta, ne pa v pisanje poročil. Predlagamo, da se poročila omejijo na najnujnejša potrebna;
-opredeli pomen pojmov »finančne izgube«, »precejšnje premoženjske ali nepremoženjske škode« in »domnevno povzročen z nezakonitim ali zlonamernim dejanjem«.

K navedenim predlogom in pripombam Sekcije operaterjev elektronskih komunikacij (SOEK) prilagamo Prilogo 1: Informacijski sistem, namenjen zajemu podatkov obvestil in poročil operaterjev o dogodkih (dokument, ki ga je dne 20. 5. 2024 Združenje za informatiko in telekomunikacije pri GZS posredovalo Agenciji za komunikacijska omrežja in storitve RS).

Glede na navedene strokovne argumente predlagamo, da Urad Vlade Republike Slovenije za informacijsko varnost predloge in pripombe smiselno upošteva pri pripravi nove verzije predloga Zakona o informacijski varnosti. Za dodatna pojasnila in nadaljnje sodelovanje smo vam na voljo.

S spoštovanjem,

Nenad Šutanovac
Direktor Združenja za informatiko in telekomunikacije pri GZS

NENAD ŠUTANOVAC
Digitalno podpisal NENAD ŠUTANOVAC
Datum: 2024.06.05 09:24:20 +02'00'

Vesna Nahtigal
Generalna direktorica

VESNA NAHTIGAL
Digitalno podpisal VESNA NAHTIGAL
Datum: 2024.06.05 12:49:43 +02'00'

Priloga 1: Informacijski sistem, namenjen zajemu podatkov obvestil in poročil operaterjev o dogodkih (dokument, ki ga je dne 20. 5. 2024 Združenje za informatiko in telekomunikacije pri GZS posredovalo Agenciji za komunikacijska omrežja in storitve RS).