Urad Vlade Republike Slovenije za informacijsko varnost
Ulica gledališča BTC 2
1000 Ljubljana

Ljubljana, 18. 3. 2024

Zadeva: **Pripombe k osnutku predloga Zakona o informacijski varnosti (EVA 2023-1544-0005)**

Zveza: **Objava na eDemokracija, 16.2.2024**

Spoštovani,

V Sekciji operaterjev elektronskih komunikacij pri Združenju za informatiko in telekomunikacije, Gospodarska zbornica Slovenije, smo proučili predlog **osnutka Zakona o informacijski varnosti (EVA 2023-1544-0005)**, h kateremu podajamo pripombe v nadaljevanju. Izrecno poudarjamo, da se članica SOEK, družba Telekom Slovenije, d.d, Cigaletova 15, Ljubljana, ne pridružuje predmetnim pripombam. **Pripombe podajajo zgolj članice SOEK, družbe A1 Slovenija, d.d., Telemach Slovenija, d.o.o.., in T-2, d.o.o.**

I. Splošno

1. Obdobje javnega posvetovanja

Uvodoma ugotavljamo, da je bil rok za pregled tega izredno pomembnega zakona, prekratek za podroben pregled. Izražamo upanje, da se bo na podlagi prejetih pripomb, izvedla ustrezna javna predstavitev zakona, ker je verjetno, da imamo deležniki, ki se nas zakon neposredno tiče vsebinsko različne pripombe ter bo vse interese težko uskladiti, da bo zakon enako veljal za vse.

Naslovni organ naj po preučitvi vseh pripomb in premisleku kako jih implementirati, izvede javno predstavitev zakona ter omogoči dodatno razpravo, ki je po našem mnenju še kako potrebna, saj je predlog zakona v tem trenutku še presplošen za natančnejše komentiranje. Časa za premišljen prenos direktive NIS2 je dovolj (24. 10. 2024).

2. Področje uporabe zakona (3. člen)

Zelo pomembno je, da se natančno in nedvoumno opredelijo obveznosti, ki jih morajo upoštevati subjekti. Zato opozarjamo, da je 3. člen nekoliko nerazumljiv, ker uvodoma (1. in 2. odst.) opredeljuje zavezance, nato v 9. odstavku naredi izjemo, pri čemer opozarjamo, da so bistveni subjekti npr. lahko hkrati kritična infrastruktura, zavezani k določenim obveznostim glede informacijske varnosti.

Nujno je treba bolje opredeliti kaj pride v poštev v takšnih primerih – »po učinku enakovredni« je bilo strokovnjakom s tega področja nerazumljivo.

Dalje opozarjamo tudi, da je treba za posamične subjekte natančneje opredeliti kaj za njih velja – s tem imamo v mislih operaterje elektronskih komunikacijskih omrežij, ki praviloma z informacijsko (ali kibernetsko) varnostjo nimajo neposredne povezave, če zagotavljajo samo pasivno infrastrukturo. Operaterji, ki najemamo takšna omrežja, v internih varnostnih dokumentih poskrbimo, da se ustrezno naslovijo zunanja tveganja, kamor sodijo tudi omrežja v najemu.

3. Obrazložitev posamičnih členov

Kot smo omenili, je predlog zakona mestoma zelo nejasen, zato smo pojasnila skušali poiskati v obrazložitvi, kar se je izkazalo za popolnoma nemogoče.

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 ustrezno dopolnijo in pojasni smisel ter namen posamične norme.

4. Vitalni interesi Slovenije

V predlogu zakona (peti odstavek 4. člena predloga), se pojavlja obveznost, da se podatki in informacije, ki se obdelujejo po tem zakonu in so vitalni za nacionalni interes, ne smejo iznašati izven Republike Slovenije.

Opozarjamo, da je takšna opredelitev presplošna, iz obrazložitve sploh ni mogoče razbrati nič več kot je napisano v samem členu, kar je v konkretnem primeru izredno kritično. Eden zelo prisotnih trendov je t.i. oblačenje, ki fizično raven sistemov seli neposredno v oblak, oblak pa na komunikacijsko infrastrukturo predvsem na strežnike na območju EU/EEA.

Na tem mestu posebej izpostavljamo določbo 23. člena ZVOP-2, ki je nacionalna določba in obveznost tovrstnega urejanja ne izhaja iz Splošne uredbe o varstvu podatkov 2016/679. V določbi 4. odstavka zadevnega člena je določeno, katerih zbirk osebnih podatkov ni dovoljeno hrani izven ozemlja Republike Slovenije.

Menimo, da je vitalnega pomena za varnost Republike Slovenije, da se natančno in določno opredeli kateri sistemi tre izrecno tudi katere kategorije (osebnih) podatkov se morajo nahajati na območju Republike Slovenije (npr. sistemi kjer se obdelujejo tajni podatki, prometni podatki, lokacijski podatki, podatki potrebni za izvajanje zakonitega prestrezanja, prisluhov,…).

Kako bo organ to nadzoroval in kaj v primeru zatečenega stanja?

II. K posamičnim določilom v predlogu zakona

5. člen (pomen izrazov)

10. Informacijska varnost: Ta definicija je drugačna kot v ZEKom-2. Ali je kakšen poseben razlog za to?

13. Kibernetska higiena: Opredelitev ne pove ničesar in je popolnoma neopredeljena ter presplošna. Enako tudi izrazi *16. Kibernetski prostor, 17. Kibernetska varnost in 18. Ključni deli nacionalnegavarnostnega sistema.*

14. Kibernetski incident velikih razsežnosti: Ta definicija je drugačna kot v ZEKom-2. Ali je kakšen poseben razlog za to?

49. *Skorajšnji incident*: Kaj je s tem zajeto. Kaj je skorajšnji incident? Na to se nihče ne more pripraviti, ali tega pričakovati. Zakaj je takšno nedorečeno izrazoslovje potrebno?

6. člen (zavezanci), 2. odstavek, 6. točka

Kdo konkretno je mišljen z izrazom »subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo«? Namreč v Zakonu o kritični infrastrukturi sta opredeljena Upravljavec kritične infrastrukture in Nosilec sektorja.

7. člen (samoregistracija in seznam zavezancev)

Če je subjekt že registriran kot kritična infrastruktura, ali se mora registrirati ponovno?

15. člen (sodelovanje skupin CSIRT z deležniki zasebnega sektorja)

Na več mestih se omenja sodelovanje CSIRT z deležniki iz zasebnega sektorja.

Glede na pooblastila ki jih imajo CSIRT po tem zakonu, podatki , ki jih nadzorujejo ali imajo do njih dostop, med drugim do najbolj varovanih področij posamičnega subjekta, ostro nasprotujemo tako neopredeljenemu sodelovanju z »deležniki zasebnega sektorja«, ne da bi se opredelil položaj in pooblastila teh zasebnih deležnikov.

Takšno sodelovanje mora biti omejeno, absolutno ne sme omogočati dostopa do varovanih podatkov nadzorovanih subjektov, sodelovanje mora biti transparentno, podvrženo ustrezni redni kontroli, kar je najmanj kar je treba zagotoviti v tem zakonu.

Sem verjetno spada tudi sklepanje sporazumov organa z gospodarskimi družbami , kar je deloma razumljivo, saj bodo gospodarske družbe lahko pripevale dragocene izkušnje in orodja, kar organu z omejenim proračunom ne bo omogočeno, a naj opozorimo še enkrat, da

tak pomočnik ne bo smel imeti dostopa do podrobnosti, ki jih organu posreduje subjekt oz. lahko do njih preko pooblastil dostopa organ.

IV. poglavje Ukrepi za obvladovanje tveganj in priglasitve incidentov

Kot smo opozorili uvodoma, smo operaterji povrženi strogi in natančno opredeljenim pravilom glede zagotavljanja varnosti v najširšem pomenu, in sicer z ZEKom-2 in na njegovi podlagi izdanimi podzakonskimi predpisi. Sistem je vpeljan že več kot desetletje, preizkušen in zanesljiv.
Tako v predmetnem predlogu zakona pogrešamo večjo opredeljenost naših obveznosti, trenutno je zakon zelo nedorečen in ni jasno kaj konkretno se od subjektov pričakuje.

V 20. členu je opredeljeno, da Vlada lahko izda predpis – menimo, da ta obveznost ne sme biti fakultativna, pač pa je izdaja tega predpisa, ki bo konkretiziral obveznosti, obligatorna.

25. člen (obveznost priglašanja in obveščanja)

5. odstavek:

Predlagamo konkretnejšo opredelitev vseh potrebnih informacij, ki jih je potrebno sporočiti.

6. odstavek:

Kaj pomeni »Kadar je ustrezno« in kdo so »prejemnike svojih storitev«, ki jih je treba obvestiti?

26. člen (postopek priglasitve pomembnih incidentov)

Upoštevaje, da sistem obveščanja za operaterje elektronskih komunikacij ni nov, bi predlagali, da se v čim večji meri ognemo težavam pri implementaciji, da se ohrani ureditev, ki je v veljavi že danes ter je opredeljena v ZEKom-2.

Predlagamo, da se, v kolikor organ nima dežurne službe, rok za obveščanje opredeli »naslednji delovni dan«.

Predlagamo tudi da se poenostavijo obveščanja, ker predlog zakona brez razlage zahteva ogromno poročanja, pri čemer so v primeru incidenta, prizadevanja subjektov usmerjena v odpravo incidenta, ne pa pisanje poročil, kar je menda organu razumljivo. Predlagamo, da se v celoti ohrani sistem opredeljen z ZEKom-2 ter splošnim aktom o obveščanju in vrednotenju incidentov ter se poročila omejijo na najnujnejša potrebna. Predvsem pa naj se vzpostavi platforma za avtomatizirana poročanja – naj izpostavimo da smo se v dolgi vrsti let upoštevanja obveznosti ki so opredeljene z ZEKom-2, operaterji izpopolnili sistem obveščanja in predmetni zakon preveč ter brez nujne obrazložitve zakaj, posega v to.

Ni tudi jasno kaj pomeni »domnevno povzročen z nezakonitim ali zlonamernim dejanjem« - kako organ ocenjuje, da bi to ugotavljali?

32. člen (vrednotenje incidenta in ukrepanje)

Ustna odločba: Predlog zakona v nujnih primerih predvideva možnost izdaje ustne odredbe. Kdaj v tem primeru bo izdana pisna odločba (zoper katero je možno pravno sredstvo)? Predlagamo, da se navedeno doda.

Menimo tudi, da bi bilo nujno potrebno tudi natančneje opredeliti v katerih primerih se lahko izda ustna zahteva, predvsem pa velja, da ko se odredijo ukrepi, morajo biti tui sorazmerni in primerni, ker bi se želeli izogniti pretiranim zahtevam, ki niso potrebne in povzročajo nesorazmerne stroške. V primeru pretiranega in nerazumnega stroška, pa lahko ukrep, če organ oceni da je potreben, financira neposredno organ, sploh če so npr. ogroženi vitalni interesi države.

Odredba: Zakaj je odredba potrebna in kaj se z odredbo lahko naloži, ker to ni urejeno in je za razumeti, da se lahko naloži vse kar si organ zamisli, ne glede na potrebnost, razumnost, stroške, čemur seveda ostro nasprotujemo. Zakaj se v tem primerih ne izda odločba, zoper katero je možno pravno sredstvo, ki kot kaže zoper odredbo ni mogoče, kar je v nasprotju s pravnim redom Republike Slovenije, v katerem so možne instančne presoje vsakega oblastnega akta države? Predlagamo, da se to določilo 7. odstavka črta kot nepotrebno.

33. člen (ocena ogroženosti)

Kako, ter ob upoštevanju katerih kriterijev se izvede vrednotenje incidentov, kot je opredeljeno v 1. odstavku?

Ko bo stopnja ogroženosti visoka ali celo kritična, bo to verjetno pomenilo, da je nastopilo izredno stanje - stanje ogroženosti, kjer pa je za operaterje elektronskih komunikacij že potrebno upoštevati tudi določila področnega zakona ZEKom-2, kar je treba ustrezno urediti.

Dalje se v 6. odstavku predvideva »spremljanje celotnega prometa“ – prosimo za pojasnilo kaj naj bi to pomenilo, glede na to, da so določeni ukrepi v Sloveniji izrecno prepovedani in so usmerjeni v spremljanje vsebine prometa (t.i. DPI). Iz obrazložitve ne razberemo kaj naj bi ta ukrep pomenil in kako naj se izvaja.

7. in 8. odstavek nista smiselna za zelo nizko in nizko stopnjo ogroženosti, mnenja pa smo, da se lahko izvajata zgolj, če ukrepi iz 6. odstavka niso zadostni, kar bi bilo potrebno tako opredeliti.

9. odstavek uvaja ukrep, ki po naši oceni najverjetneje ni potreben, saj so tveganja zadostno naslovljena s 6. odstavkom, ter nato 7. in 8. odstavkom. Predlagamo, da se določilo črta ter se namesto tega raje uredi, da se organ in CERT medsebojno strinjata kaj je potrebno ter se to uredi z enim aktom – celostno, koordinirano, premišljeno in zgolj kar je potrebno, nujno in sorazmerno s tveganjem.

41. člen (nadzor bistvenih subjektov)

Menimo, da priložnostne revizije niso potrebne, če ima subjekt letna poročila o reviziji, ki po naši oceni zadostujejo za izvedo nadzora.

Predlagamo, da se revizija uredi po vzoru 123. člen ZEKom-2 ter se navedeno določilo smiselno ter v celoti povzame v predmetni zakon.

XI. Prehodne določbe

V prehodnih določbah se večkrat omeni, da veljavni podzakonski predpisi veljajo do izdaje novih.

Predlagamo, da se v odzivu na pripombe natančno navede kateri novi podzakonski predpisi bodo izdani na podlagi predmetnega zakona, saj je to nekoliko težko ugotoviti.

Prav tako predlagamo, da se predvidi ustrezne prehodni rok za vse primere, da subjekti v času uveljavitve niso skladni s tem zakonom in bi morali to nedoslednost odpraviti, pa gre za velik, obsežen sistemski poseg – predlagamo najmanj 7 let, po vzoru 312. člena ZEKom-2.

Za pojasnila ostajamo na razpolago. Kot smo predlagali uvodoma, bi bila zaradi daljnosežnih posledic, ki jih prinaša ta zakon, potrebna previdnost in premišljenost – naslovni organ naj se opredeli do prejetih pripomb, izvede javno predstavitev predloga zakona, po preučitvi pripomb, zaradi katerih bi bilo potrebno prilagoditi obstoječi predlog, pa izvede še eno posvetovanje. Časa je vsekakor dovolj.

S spoštovanjem,

Martina Ferjančič, predsednica SOEK

Nenad Šutanovac, direktor
Združenje za informatiko in telekomunikacije pri GZS