REPUBLIKA SLOVENIJA
DRŽAVNI SVET
Komisija za državno ureditev

Številka: 011-02-2/2018/6 EPA 2594-VII
Ljubljana, 5. 4. 2018

Komisija Državnega sveta za državno ureditev je, na podlagi drugega odstavka 56. člena Zakona o Državnem svetu (Uradni list RS, št. 100/05 - uradno prečiščeno besedilo, 95/09 – odl. US, 21/13 - ZFDO-F) in 20. člena Poslovnika Državnega sveta (Uradni list RS, št. 70/08, 73/09, 101/10, 6/14 in 26/15), sprejela naslednje

M n e n j e

k Predlogu zakona o informacijski varnosti (ZInfV) – druga obravnava

Komisija za državno ureditev (v nadaljevanju: komisija) je na 5. seji 7. 3. 2018 obravnavala Predlog zakona o informacijski varnosti, EPA 2594-VII (v nadaljevanju: predlog zakona), ki ga je v obravnavo Državnemu zboru predložila Vlada Republike Slovenije (v nadaljevanju: predlagatelj).

Komisija **podpira** predlog zakona.

* * *

Evropska unija (EU) je 2016 sprejela Direktivo o ukrepih za visoko raven varnostnih omrežij in informacijskih sistemov in na tej podlagi je pripravljen predlog zakona. Z njim se želi povečati raven informacijske varnosti v Republiki Sloveniji in v EU. Uresničevanje predloga zakona bo zagotovilo visoko raven varovanja omrežij in informacijskih sistemov, ki so bistvenega pomena za nemoteno delovanje države in s katerimi se zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti. Predlog zakona vzpostavlja minimalne varnostne zahteve, prav tako pa tudi zahteve za priglasitev incidentov in pristojnosti, naloge in organizacijo odgovornega nacionalnega organa, ki bo oblikovan kot organ v sestavi ministrstva pristojnega za informacijsko družbo. Predlog zakona predvideva tudi

enotne kontaktne točke, nacionalne skupine za obravnavo incidentov in pa skupino za obravnavo incidentov v organih državne uprave.

Po predlogu zakonu bodo zavezanci izvajalci bistvenih storitev z naslednjih področij: energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura bančnega trga. V naši različici predloga zakona sta na seznam bistvenih storitev vključena še preskrba s hrano in varstvo okolja, kar se sklada z Zakonom o kritični infrastrukturi. Organizacije, zavodi oziroma podjetja, ki bodo prepoznani kot izvajalci bistvenih storitev bo določila uredba, ki jo bo sprejela Vlada na podlagi priporočil, ki jih bo pripravila EU. Po predlogu zakona bodo zavezanci tudi ponudniki digitalnih storitev, to so spletne tržnice, spletni iskalniki in računalništvo v oblaku. Gre za zavezance, ki jih je določila evropska direktiva, po našem predlogu zakona pa bodo zavezanci tudi organi državne uprave. Zavezanci bodo morali v skladu z zakonom poleg ključnih varnostnih zahtev voditi tudi posebno varnostno dokumentacijo in sprejemati določene varnostne ukrepe. Predviden je način priglasitve incidentov in določeni so organi, ki jim bo treba poročati o zaznanih incidentih. Predlog ureja tudi nadzor nad izvajanjem zakona, ki ga bodo opravljali inšpektorji za informacijsko varnost. Naloge informacijske varnosti bo do 1. januarja 2020 opravljal Urad za varovanje tajnih podatkov, od takrat naprej pa nacionalni organ v sestavi ministrstva pristojnega za informacijsko družbo. Vseh finančnih posledic predloga zakona še ni bilo mogoče predvideti, saj so na ravni zakona našteti zgolj sektorji, ki se jih zakon dotika, medtem, ko bodo zavezanci s posameznih sektorjev določeni šele na podlagi vladne uredbe. Merila bodo šla v smer, da pride npr. v poštev banka, ki bo imela določeno število komitentov ali osnovnega kapitala v povezavi z BDP. V poštev bo prišlo komunalno podjetje, ki ima določeno število uporabnikov, zdravstveni dom, ki ima večje število pacientov in tako naprej. EU želi, da imajo vse države področje urejeno enotno. Predlog zakona želi dvigniti splošen nivo zavedanja o pomenu zagotavljanja informacijske varnosti, področju v zadnjih letih ni bilo namenjeno dovolj pozornosti. Vladna uredba mora biti pripravljena v roku 6 mesecev po sprejetju zakona, Ministrstvo za javno upravo (MJU) bo uredbo dalo v javno obravnavo in različni deležniki, tudi lokalne skupnosti, bodo imeli možnost sodelovati pri njenem nastajanju in nastajanju meril za določitev kriterijev za zavezance.

Komisija je bila seznanjena z mnenjem Zakonodajno-pravne službe Državnega zbora (ZPS) in z mnenjem Združenja občin Slovenije (ZOS).

* * *

V razpravi so državni svetniki izpostavili pomen informacijske varnosti in krepitve zavesti o tem področju. Gre za nujne ukrepe, s kateri že zamujamo, glede na to, da ni več nobenega poslovnega procesa, ki ne bi bil podprt z informacijsko tehnologijo. Člani komisije so se strinjali, da bodo zahteve in naloge za zavezance pospešile zavedanje podjetij in zaposlenih, da potrebujejo nova znanja s področja informacijske varnosti. Na komisiji je bila dana primerjava, da imamo glede požarne varnosti in zaščite pri delu stalna usposabljanja, medtem, ko jih na področju informacijske varnosti nimamo. Zato bo treba poleg ustrezne zakonodaje vzpostaviti tudi stalno osveščanje o pomenu informacijske varnosti. Komisija je menila, da je predlog zakona nujen odziv na razmere v svetu in pri nas, saj smo brez ustrezne zaščite

ranljivi in izpostavljeni kibernetskim napadom. Predlog zakona je, kot so dejali člani komisije, nekakšen »stres test« za sisteme v državi, da se bodo bolj zavedali nevarnosti in se bodo znali ustrezno odzivati na incidente. Predlagatelj je na komisiji izpostavil 27. člen predloga zakona, ki govori o pristojnem nacionalnem organu, ki bo moral v skladu s 7. točko koordinirati usposabljanja, vaje in izobraževanja o informacijski varnosti in skrbeti za dvig zavedanja javnosti o pomenu in načinih informacijske varnosti.

Na komisiji so bila predlagateljem zastavljena tudi vprašanja glede odgovornosti za zagotavljanje informacijske varnosti in kaj je z odškodninsko odgovornostjo podjetij in zavodov, če pride do kibernetskih vdorov in morebitnih odtujitev osebnih podatkov uporabnikov storitev (zdravstvene storitve, komunalne storitve in drugo), ali predlog zakona predvideva kakšne sankcije za neizvajanje varnostnih standardov. Ali ta predlog zakona sam po sebi prinaša kakšno direktno zaščito za potrošnika v primeru zlorabe podatkov, do katerih bi prišlo zaradi kibernetskih napadov in ali ima podjetje ali institucija do posameznika kakšno odškodninsko odgovornost, ker je slabo zaščitila njihove podatke? Člani komisije so opozorili še na dodatno dimenzijo kibernetske varnosti, ključni igralci, ki imajo nadzor nad prometom informacij so izven naše države in je zato vprašanje, kako samostojni smo pri zagotavljanju informacijske varnosti? Predlagatelj je v zvezi z navedenimi vprašanji članom komisije pojasnil, da je za informacijsko varnost najprej odgovoren vsak organ zase. Kot je za vsako organizacijo pomembno vodenje financ ali kadrovskih vprašanj, bo morala postati pomembna tudi odgovornost za izvajanje postopkov za informacijsko varnost in zavedanje vsakega organa, da bo moral poskrbeti za informacijsko varnost svojih sistemov. V večini primerov se namreč izkaže, da do posameznih incidentov prihaja zaradi človeške napake zaposlenih (neurejen sistem gesel, nedefinirano posodabljanje sistemov…). Za zmanjšanje ali odpravo teh napak pa mora skrbeti vsak organ zase, tega ne more zagotavljati država. Država mora urediti zakonodajni del, ki predstavlja sistematičen okvir delovanja in koordinacijo celotnega sistema na enem mestu. Prav tako mora država skrbeti za višanje osveščenosti o pomenu informacijske varnosti, saj se sistemi povezujejo med seboj in informacijska tehnologija je vpeta v vedno več delovnih procesov. Predlagatelj je v skladu z 11. členom predloga zakona še poudaril, da bo moral vsak zavezanec narediti ocenjevalni postopek in preko njega preveriti stanje svojega informacijskega sistema in na osnovi tega stanja pripraviti varnostno dokumentacijo, ki bo morala vsebovati mehanizme preprečitve kibernetskih vdorov in imeti za primere incidenta izdelane postopke ravnanj. V primeru incidenta je največja napaka, da ne vemo kako ukrepati, koga obveščati, kakšna je linija poročanja in kdo je odgovoren za kaj. Po mnenju predlagatelja je izjemno pomembno, da se zaznajo tudi vse grožnje in nameni za incidente in se o tem poroča organom in centralni enoti in tako se tudi drugi sektorji zavedajo groženj in se nanje ustrezno pripravijo in okrepijo varnost. Ta predlog zakona je v prvi vrsti namenjen preventivi in ne toliko kurativi. Predlog zakona stremi k temu, da se na tem področju uveljavi resno in sistematično delo, saj se z digitalizacijo družbe možnost za kibernetske napade povečuje in moramo pripraviti ustrezno obrambo. V zvezi z direktno odgovornostjo, tudi finančno oziroma odškodninsko posameznih podjetij oziroma ustanov, pa je bilo s strani predlagateljev izpostavljeno 11. poglavje predloga zakona - kazenske določbe, ki pravi, da mora vsak zavezanec narediti celoten postopek ocene in predvidenih ukrepov, v tem delu so tudi specificirane globe, če zadeve niso izvedene ali niso ustrezno izvedene. Sankcije so predvidene, vendar pa je predlog zakona bolj usmerjen v ozaveščanje

zavezancev in javnosti o pomenu informacijske varnosti. Predlagatelj je pojasnil, da predlog zakona ne ureja pravic potrošnikov, saj ta izhaja iz zakonodaje o varstvu potrošnikov, seveda pa nihče ne izključuje splošnih pravil o odškodninski odgovornosti. Predlog zakona vzpostavlja sistem informacijske varnosti preko določanja zavezancev, ki so odgovorni zanjo.

Na komisiji je bilo postavljeno tudi vprašanje ali so predpisi s področja informacijske varnosti usklajeni s predpisi in dolžnostmi, ki izhajajo iz sprememb zakonodaje na področju varstva podatkov, ki bodo veljali na mednarodni ravni, kjer je tudi predpisanih precej ukrepov in nalog. Predlagatelj je članom komisije zagotovil, da so predpisi med seboj usklajeni. V 3. členu predloga zakona je tako definirana obdelava podatkov in da vsaka obdelava osebnih podatkov poteka v skladu s trenutno veljavnim Zakonom o varovanju osebnih podatkov. Enako kot evropska direktiva, ki se jo prenaša s tem predlogom zakona, se tudi predlog zakona sklicuje na splošno uredbo in evropske predpise o varstvu osebnih podatkov in na direktivo, ki je trenutno prenesena z Zakonom o varstvu osebnih podatkov, pa tudi na splošno uredbo o varstvu osebnih podatkov EU, ki je neposredno uporabljiva.

Člane komisije je zanimalo ali bodo med zavezance za digitalne storitve vključena tudi podjetja, ki se ukvarjajo s kripto valutami, pri katerih je zaradi kibernetskih napadov že prišlo do določenih škod. Komisija je razmišljala tudi o stroških, ki jih bo imelo gospodarstvo s prilagoditvijo predlogu zakona, saj jih bo izvajanje ukrepov dodatno obremenjevalo in kakšna bodo za podjetje administrativna bremena za izpolnjevanje zahtev iz predloga zakona. Člani komisiji so še izpostavili, da je v proračunu za 2018 za večanje informacijske varnosti namenjeno 530.000 evrov in jih je zanimalo za kaj točno se bodo ta finančna sredstva porabila. Predlagatelj je glede zavezancev z digitalnega področja članom komisije pojasnil, da gre v tem primeru predvsem za podjetja, ki delujejo na globalnem trgu in ponujajo oblačne storitve, spletne tržnice ali pa spletne iskalnike, vendar je teh ponudnikov v Sloveniji zelo malo. Prav tako spisek zavezancev še ni znan, ker se šele pripravlja uredba, ki bo določila merila za izbor zavezancev. Glede podjetij, ki se ukvarjajo s kripto valutami je bilo s strani predlagatelja opozorjeno, da v primeru, če bi takšno podjetje sodilo med zavezance, bo moralo zagotavljati enake varnostne standarde kot drugi. Predlagatelj se je sicer strinjal, da zagotavljanje informacijske varnosti nekaj stane, vendar se je treba zavedati, da so kibernetski napadi še mnogo dražji in da je treba vlagati finančna sredstva v dvig informacijske varnosti. Predlog zakona zato zelo poudarja pomen osveščanja javnosti in zavezancev. Višja raven informacijske varnosti je lahko tudi konkurenčna prednost EU pred drugimi območji sveta. Predlagatelj je pojasnil, da so predvidena finančna sredstva v višini nekaj več kot 500.000 evrov namenjena vzpostavitvi enotnega nacionalnega organa za skrb nad informacijsko varnostjo, del sredstev pa bo namenjen nakupu programske opreme za višanje nivoja varnosti na področju informacijsko-komunikacijskih sistemov v državnih organih. Z novo zakonodajo se želi čim manj administrativno obremenjevati podjetja in druge zavezance, zato se je pri vseh obveznostih predvideva, da v kolikor imajo zavezanci varnostno dokumentacijo že pripravljeno na podlagi druge zakonodaje - o kritični infrastrukturi, varstvu osebnih podatkov itd., potem jo skladno s tem zakonom samo dopolnijo. Velike družbe, podjetja in organizacije, ki bodo v večini tudi zavezanci, imajo v glavnem te stvari že dobro urejene in bo šlo samo za manjše dograditve sistema.

Komisijo je zanimalo ali je bila pred samo pripravo predloga zakona pripravljena kakšna analiza stanja glede informacijske varnosti znotraj državnih organov (npr. na upravnih enotah, ki izdajajo biometrične potne listine, varnost elektronskih podpisov…) in v zasebnem sektorju. Predlagatelj je ravno v zvezi s tem vprašanjem članom komisije posebej izpostavil, da evropska direktiva organov državne samouprave ne vključuje med zavezance, pri nas pa smo zaradi zavedanja, kako šibki smo na tem področju varnosti, vključili med zavezance tudi organe državne uprave. Gre za nacionalno določbo, ker se želimo sistematično lotiti dela v tem sektorju. Glede analiz stanja informacijske varnosti predlog zakona vsebuje t.i. test MSP (test malih in srednjih podjetij), preko katerih se je ocenjevalo ustreznost nivoja informacijske varnosti (ocenjevalo se je 300 gospodarskih subjektov, od tega je bilo 75 ocenjenih kot neustreznih), kar daje nek vpogled v situacijo. Posledično je v MSP testih ocenjen tudi strošek za izboljšanje informacijske varnosti in se ga ocenjuje na približno 2 milijona evrov, kar ni velik strošek, glede na morebitno škodo v primeru kibernetskih incidentov. Informatika organov državne uprave se centralizira, določeni organi so že bili ali pa bodo centralizirani, kar bo pripomoglo k višji stopnji varnosti. Na MJU se gradijo 3 oblaki infrastrukture - državni oblak, hibridni oblak in oblak za razvoj in raziskave in v sklopu državnega računalniškega oblaka so določena ministrstva že centralno vsebovana (podatki, aplikacije…) in v tem delu je nivo informacijske varnosti zadovoljiv.

Na komisiji je bilo glede informacijske varnosti in preverjanja le-te predstavljen tudi primer eAsistent, ki se uporablja v izobraževanju in preko katerega se vodi mnogo osebnih podatkov učencev, pri tem pa je podjetje, ki je lastnik eAsistenta zasebno podjetje. Postavlja se vprašanje, kdo je odgovoren, če pride do razkritja ali uničenja podatkov, če portal eAsistent ne bi bil dovolj dobro zavarovan pred kibernetskimi napadi. Predlagatelj je izpostavil, da gre v tem primeru v prvi vrsti za problem varovanja osebnih podatkov in je vprašanje, če bo ta sistem po uredbi sodil med zavezance za informacijsko varnost. Vsekakor pa predlog zakona tudi takšne sisteme skuša osveščati in opozarjati na potrebo po večji skrbi in odgovornosti vsakega subjekta za informacijsko varnost, saj so posledice lahko izredno boleče in na številnih področjih.

Komisija je v zvezi s poslanimi pripombami na predlog zakona s strani Združenja občin Slovenije opozorila na finančne posledice za lokalne skupnosti in na neurejeno usklajevanje povprečnin ter na nove obremenitve lokalnih skupnosti, čeprav je bila obljubljena celo njihova razbremenitev. V končni točki lahko del obremenitev pade tudi na porabnike javnih storitev, če bodo določena javna podjetja sodila med zavezance in bodo morala večja finančna sredstva vložiti v izboljšanje informacijske varnosti. Tudi ostala podjetja, ki bodo postala zavezanci lahko del stroškov prevalijo na uporabnike storitev, komisija se je strinjala, da to ni prav. Predlagatelj ni zanikal, da do določenih finančnih posledic bo prišlo, ponovljeno pa je bilo, da trenutno še ni narejen spisek zavezancev in zato vseh finančnih posledic v predlogu zakona ni bilo mogoče ovrednotiti. Moramo pa se zavedati, da lahko en kibernetski napad organizacijo stane več, kot pa je celoten strošek za zagotavljanje informacijske varnosti. V začetku bodo finančne posledice večje, ker bo treba pripraviti oceno tveganja in popisati celoten informacijski sistem, vzpostaviti sistem ukrepanja, določiti odgovorno osebo v sami organizaciji, ki bo odgovorna za poročanje, vse skupaj pa bo moralo postati del samega vodenja organizacije, da bo zagotovila minimalne

varnostne standarde, vendar je odpravljanje posledic težje in dražje, kot pa pravočasno ukrepanje.

* * *

Za poročevalca je bil določen državni svetnik Rajko Fajt.

Rajko Fajt, l.r.
predsednik