REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Št.: 010-4/2017/18
Datum: 10. 8. 2017

Ministrstvo za javno upravo
gp.mju@gov.si

Zadeva: Mnenje Informacijskega pooblaščenca glede predloga Zakona o informacijski varnosti

Spoštovani,

zahvaljujemo se vam za predlog Zakona o informacijski varnosti (verzija z dne 4. 8. 2017; v nadaljevanju ZIV), ki ste nam ga posredovali v podajo pripomb.

Informacijski pooblaščenec (v nadaljevanju IP) uvodoma pojasnjuje, da je v okviru Medresorske delovne skupine za pripravo zakona o kibernetski/informacijski varnosti glede predvidene obvezne hrambe že večkrat izdatno opozoril na spornost takšnih določb, zadnjič v mnenju št. **010-4/2017/7 z dne 6. 6. 2017.** V nadaljevanju na podlagi 48. člena Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 86/04, 113/05, 51/07 in 67/07, v nadaljevanju ZVOP-1) podajamo naše pripombe na zadnje prejeto besedilo po členih predloga zakona.

K 3. členu

Splošna in vsebinsko prazna določba 1. odstavka 3. člena: »*Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno z zakonom, ki ureja varstvo osebnih podatkov.*« se nam ne zdi potrebna, in v njej ne vidimo dodane vrednosti. Če določena zakonodaja že postavlja pravila na določenem področju, ni potrebno, da se nanjo posebej napotuje, saj velja tudi brez takšnih napotitev. Bistveno pa seveda je, da zakon ustrezno ureja področje pridobivanja in drugih oblik obdelave osebnih podatkov v zvezi z izvajanjem zakona, na kar opozarjamo v nadaljevanju. Sama splošna določba namreč temu ne zadosti.

V drugem odstavku 3. člena ni jasno, kaj (vse) so »*informacije, ki so zaupne v skladu s predpisi EU in nacionalnimi predpisi*«, saj ne zasledimo njihove definicije. Gre za osebne podatke, tajne podatke, poslovne skrivnosti, ali vse našteto? Pojem »zaupne informacije« je sicer vsebinsko lahko nadpomenka naštetim, a menimo, da bi moral biti natančneje opredeljen.

Če je namen predlagatelja, da definicija tega pojma zajema tudi varovane osebne podatke, določba z vidika sorazmernosti poseganja v ustavno varovano pravico do varstva osebnih podatkov ni ustrezna. Posredno namreč določa, da se lahko najrazličnejše, torej dejansko katerekoli (ni določen nabor), »*zaupne informacije*« izmenjajo z Evropsko komisijo in drugimi ustreznimi organi (ti niso jasno in izključno oz. vnaprej predvidljivo določeni) vedno, kadar je takšna izmenjava potrebna na podlagi tega zakona. Vsem pristojnim organom je torej prepuščena prosta presoja o tem, kateri so ustrezni organi, ki lahko na ta način pridobijo katerekoli informacije, če so te po oceni ustrezne in sorazmerne glede na namen ter iz katerih zbirk (torej bodisi javnih evidenc ali zbirk vseh drugih upravljavcev). Pri čemer je zakonsko opredeljen namen za upravičevanje tovrstnih najrazličnejših oblik obdelav (npr. pridobivanje, posredovanje, uporaba) izredno širok: »*zagotovitev visoke ravni varnosti omrežij in informacijskih sistemov Republike Slovenije, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah in zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti*«. Navedeno po mnenju IP ne zadosti zahtevam 38. člena Ustave RS glede zakonske določenosti obdelave osebnih podatkov.

Zato bi bilo po mnenju IP treba **bodisi izrecno izločiti osebne podatke iz pojma »zaupne informacije«, bodisi (kar se glede na naravo s predlogom zakona določenih postopkov zdi verjetneje) jasneje omejiti namen, nabor in upravičene uporabnike osebnih podatkov (torej za vsakega izmed z zakonom predvidenih organov posebej)**.

K 8. členu

Predlog zakona določa glede pooblastil za obdelavo osebnih podatkov le inšpekcijska pooblastila pristojnega nacionalnega organa (32. člen predloga zakona). Ta namreč upoštevajoč 19. člen Zakona o inšpekcijskem nadzoru (Ur. l. RS, št. 43/07 – uradno prečiščeno besedilo in 40/14, v nadaljevanju ZIN) med drugim vključujejo tudi pridobivanje osebnih podatkov v zvezi s posameznimi primeri nadzora. Za druge deležnike pa ni nikjer izrecno določeno, katera pooblastila imajo posamezni deležniki glede morebitnega pridobivanja in obdelave osebnih podatkov (npr. nacionalni in vladni CSIRT, pristojni nacionalni organ za obveščanje o incidentih, drugi pristojni organi držav članic ipd.). Po naravi stvari in glede na vsebino predloga zakona pa bi v okviru posameznih aktivnosti zelo verjetno lahko prišlo do tega oz. do potrebe po pridobivanju in obdelavi osebnih podatkov (npr. identifikacija imetnikov določenih IP naslovov).

Iz previdnosti zato opozarjamo, da mora biti ta materija urejena v skladu s 37. in 38. členom Ustave RS in z zakonom. Tovrstna pooblastila bi bilo torej treba za posamezne deležnike (seveda, če je to glede na zakonsko zasledovane cilje primerno, potrebno in nujno) opredeliti v zakonu (podzakonski akti kot npr. medsebojni sporazumi glede postopka obveščanja pristojnih organov iz 8. odstavka 8. člena predloga zakona ipd. ne morejo urejati te zakonske materije).

K 12. členu

Predlagani 6. odstavek 12. člena določa:

> *Zavezanci so dolžni za namen obvladovanja incidentov, skladno z izvedeno analizo obvladovanja tveganj z oceno sprejemljivega nivoja tveganj, ki jo je dolžan zavezanec izvesti po predpisani metodologiji, poskrbeti tudi za hrambo podatkov delovanja svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja, vendar ne manj kot 6 mesecev. Hramba podatkov mora biti zagotovljena na ozemlju Republike Slovenije.*

IP predlaga naslednje dopolnitve:

> *Zavezanci so dolžni za namen obvladovanja incidentov, skladno z izvedeno analizo obvladovanja tveganj z oceno sprejemljivega nivoja tveganj, ki jo je dolžan zavezanec izvesti po predpisani metodologiji, poskrbeti tudi za hrambo dnevniških zapisov o ~~podatkov~~ delovanj~~a~~u svojih ključnih, krmilnih ali nadzornih informacijskih sistemov ali delov omrežja, vendar ne manj kot 6 mesecev. Hramba dnevniških zapisov ~~podatkov~~ mora biti zagotovljena na ozemlju Republike Slovenije.*

Smiselno se popravi tudi določba 7. odstavka 12. člena:

> *V kolikor obstaja področna zakonodaja posameznega sektorja ali sistema iz 5. člena tega zakona glede hrambe dnevniških zapisov~~podatkov~~, se upošteva področna zakonodaja.*

Predlagana dopolnitev je po mnenju IP nujna za zagotovitev skladnosti določb predloga zakona s 37. in 38. členom Ustave RS in jasno razumevanje, kaj naj bi se po tej določbi hranilo. Za obvladovanje incidentov so namreč **pomembni dnevniški zapisi** (npr. podatki o (ne)delovanju določenega sistema, dostopih do (pod)sistemov itd.), **nikakor pa ne surovi, vsebinski podatki** (podatki o klicih posameznikov, diagnoze

pacientov itd.). Nobenega razloga torej ni, da bi zakonska dikcija omogočala, da se na ta način v neskladju z Ustavo RS (torej brez sodne odredbe) posega v komunikacijsko zasebnost posameznika oziroma hrani na ravni zakona neopredeljen nabor osebnih podatkov. Določbe zakona glede hrambe podatkov morajo biti natančne in **ne sme biti nobenega dvoma,** da gre v konkretnem primeru **zgolj za hrambo dnevniških datotek o delovanju pomembnih sistemov za namen obvladovanja incidentov in ne za varnostne kopije vsebinskih podatkov za namen vzdrževanja razpoložljivosti in povrnitve delovanja sistemov**. Sistem neprekinjenega poslovanja namreč že zahteva določba prvega odstavka 11. člena v povezavi z drugimi ukrepi iz 12. člena predloga zakona.

Namesto izraza »dnevniški zapisi« se lahko uporabi tudi drug ustrezen izraz, npr. revizijske sledi.

Dodatno v zvezi s tem izpostavljamo, da določba 6. odstavka 8. člena (»*Priglasitelj mora ob prijavi incidenta poskrbeti za ustrezno zavarovanje podatkov revizijskih sledi, če te obstajajo.*«) ni v skladu z zahtevo po obvezni hrambi revizijskih sledi iz 6. odstavka 12. člena.

K 19. členu

Izpostavljamo, da v tretjem odstavku 19. člena predloga zakona ni opredeljena vsebina evidenc incidentov, ki jih vodijo skupine CSIRT. Glede na to, da bi te evidence po naravi stvari lahko vsebovale tudi osebne podatke, bi morala biti npr. po vzoru prvega odstavka istega člena tudi vsebina teh evidenc zakonsko opredeljena. Lahko s sklicevanjem na vsebino evidenc iz prvega odstavka istega člena, če gre za vsebinsko primerljive evidence.

K 25. členu

Ugotavljamo, da predlog zakona v 25. členu (prav tako ne kje drugje v besedilu predloga zakona) ne vsebuje določb, o tem kaj naj bi vsebovalo tromesečno poročilo CSIRT pristojnemu nacionalnemu organu oz. ni razvidno ali naj bi ta poročila vsebovala tudi IP naslove (če bodo vsebovala podrobnejše informacije o incidentih). Glede na določbe, da poročila ne bodo vsebovala navedbe prijavitelja in če ni mišljeno, da ta poročila vsebujejo osebne podatke, predlagamo, da se to v predlog zakona zapiše npr. kot predlagamo spodaj.

»*25. člen*
(sodelovanje na nacionalni ravni)
…
(2) Nacionalni in vladni CSIRT pristojnemu nacionalnemu organu na varen način posredujeta tromesečna poročila na podlagi agregiranih priglasitev incidentov brez navedbe prijavitelja ali drugih osebnih podatkov, istočasno pa imata tudi dostop do ažurnih kontaktnih informacij zavezancev, za katere sta pristojna.
…«

K 26.-31. in 41. členu

Četudi vprašanje pravno-statusne oblike primarno ne sodi v pristojnost IP, so pa glede na izkušnje IP posredno povezana tako z učinkovitostjo zagotavljanja transparentnosti organov kot tudi s praktičnim zagotavljanjem varstva zasebnosti, na koncu zgolj v razmislek izpostavljamo vprašanje pravno-statusne oblike pristojnega nacionalnega organa. Za slednjega je namreč predvideno, da naj bi bil oseba javnega prava (ne organ v sestavi ali neodvisen državni organ), pri čemer je pravno-formalno na več mestih v predlogu zakona zaznati sklicevanje na zakon o javnih agencijah. Med drugim predlog zakona predvideva, da se pristojni nacionalni organ ustanovi z ustanovitvenim aktom, ki ga sprejme vlada na podlagi zakona, ki ureja javne agencije, in tega predloga zakona. Glede na pooblastila in naravo nalog tega organa, ki so za državo ključnega pomena, razlogi za takšno odločitev pravno gledano niso povsem razumljivi. Zakon o javnih agencijah namreč v 4. členu določa, da se javna agencija ustanovi:

- če je s tem omogočeno učinkovitejše in smotrnejše opravljanje regulatornih, razvojnih ali strokovnih nalog v javnem interesu, če zanje z zakonom ni predvidena druga statusna oblika, kot bi bilo v primeru opravljanja nalog v upravnem organu, zlasti če se lahko opravljanje upravnih nalog v celoti ali pretežno

financira z upravnimi taksami oziroma plačili uporabnikov, ali
- če glede na naravo oziroma vrsto nalog ni potreben ali ni primeren stalni neposredni politični nadzor nad opravljanjem nalog.

Javna agencija se lahko ustanovi le v primeru, ko z organizacijsko obliko organa v sestavi ministrstva ne bi bilo mogoče uresničiti cilja iz prve alinee prejšnjega odstavka.

K 35. členu

Glede na pristojnosti IP bi bilo smiselno tretji odstavek 35. člena predloga zakona dopolniti na način, da bi ta določal, ne le tesnega sodelovanja navedenih organov z IP, kadar so posledice incidentov kršitve varstva osebnih podatkov, ampak s ciljem pravočasnega ukrepanja v smeri zagotavljanja odprave kršitev tudi obvezno obveščanje IP s strani pristojnega nacionalnega nadzornega organa o primerih, kadar je bil v zvezi z obravnavanimi incidenti zaznan tudi sum kršitev varstva osebnih podatkov.

S spoštovanjem,

Informacijski pooblaščenec:
Mojca Prelesnik, univ.dipl.prav.,
Informacijska pooblaščenka

Pripravila:
- mag. Andrej Tomšič, namestnik pooblaščenke,
- Alenka Jerše, namestnica pooblaščenke.