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.: 007-69/2017/2
Datum: 9.10.2017

Ministrstvo za javno upravo
gp.mju@gov.si

Zadeva: Mnenje Informacijskega pooblaščenca glede predloga Zakona o informacijski varnosti
Zveza: Vaš dopis št. 007-644/2017/5 z dne 11. 9. 2017 in priloženo gradivo

Spoštovani,

zahvaljujemo se vam za predlog Zakona o informacijski varnosti (osnutek za javno obravnavo; v nadaljevanju ZIV), ki ste nam ga posredovali v podajo pripomb.

V skladu s svojimi pristojnostmi po 1. odst. 48. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1) v zvezi z 2. členom Zakona o informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, v nadaljevanju ZInfP) vam posredujemo mnenje Informacijskega pooblaščenca (v nadaljevanju: IP) k prejetemu predlogu Zakona o informacijski varnosti (po vašem dopisu kot zgoraj; v nadaljevanju: predlog ZIV).

Informacijski pooblaščenec (v nadaljevanju IP) uvodoma pojasnjuje, da je v okviru medresorske delovne skupine za pripravo zakona že podal svoja stališča in komentarje (zadnje v mnenju IP št. 010-4/2017/18 z dne 10. 8. 2017[1]).

Uvodoma pozdravljamo odločitev predlagatelja, da se ta zakon ne uporablja za operaterje elektronskih komunikacij, saj so s tem odpadli zadržki, na katere smo glede morebitnega ponovnega uvajanja obvezne hrambe podatkov pri operaterjih (t.i. data retention) ali celo širše, opozarjali v okviru medresorske delovne skupine.

Menimo, da je trenutni kompromisni predlog, ki obvezno hrambo omejuje na dnevniške zapise o delovanju ključnih, krmilnih ali nadzornih informacijskih sistemov (6. in 7. odstavek 12. člena), ustrezen. Kot smo že izpostavljali, namreč za namen obvladovanja incidentov ni ne potrebno ne nujno hraniti surovih, vsebinskih podatkov v bazah podatkov zavezancev, ki so pogosto osebni podatki, in s tem posegati v določbe področnih predpisov, temveč so za zasledovane namene obvladovanja incidentov pomembni *dnevniški zapisi o* delovanju, prekinitvah, neobičajnih dogodkih in drugih dogodkih v obratovanju bistvenih sistemov, iz katerih je mogoče ugotoviti in analizirati kibernetske grožnje in kibernetske napade. V izogib morebitnim napačnim interpretacijam kasneje v praksi pa priporočamo, da se to **jasno poudari v obrazložitvi k tem členu** v nadaljnji proceduri.

Prav tako iz previdnosti dodajamo, da bi veljalo v izogib kasnejšim nesporazumom v tem smislu dopolniti 8. odstavek 12. člena, na način, da se jasno določi, da pravilnik, ki naj bi podrobneje določal vsebino in strukturo varnostne dokumentacije, ne sme na novo oz. dodatno (izven vnaprej zakonsko predvidenega, bodisi v tem ali drugih zakonih) določati zbiranja in/ali obdelave osebnih podatkov. Navedeno bi bilo namreč v neskladju z 38. členom Ustave RS.

[1] https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/MJU__Mnenje_glede_Zakona_o_informacijski_varnosti_ver04-08_8avg2017.pdf

Kot smo deloma že opozorili tudi v okviru medresorske delovne skupine, iz previdnosti zgolj ponovno pripominjamo, da iz predloga zakona ni razvidno, kdo naj bi imel v zvezi z materijo, ki jo ureja predlog ZIV inšpekcijska pooblastila. Predlog ZIV govori o inšpektorju oz. inšpektorici, pristojnih za informacijsko varnost (člen 13), pri čemer pa nikjer ni opredeljeno, ali je s tem mišljeno delovno mesto inšpektorja v okviru pristojnega nacionalnega organa po členu 21 oz. v okviru katerega od drugih v predlogu zakona predvidenih organov, ali je mišljena vzpostavitev ločenega organa oz. organa v sestavi kot posebnega inšpektorata pristojnega za informacijsko varnost. Glede na to da predlog zakona med drugim vključuje tudi pridobivanje osebnih podatkov v zvezi s posameznimi primeri nadzora, bi bilo nujno, da se to ustrezno zakonsko uredi bodisi v tem ali drugem zakonu. Posameznim drugim deležnikom (predvsem npr. pristojnemu nacionalnemu organu, ki ga opredeljuje 21. člen predloga zakona) namreč predlog zakona izrecno ne podeljuje inšpekcijskih pooblastil. Ta so podeljena samim inšpektorjem.

Dodatno v zvezi z 19. členom glede vodenja seznamov po tem členu in v povezavi s 23. členom predloga zakona, ki predvideva vzpostavitev vladnega CSIRT-a, izpostavljamo, da si člena vsebinsko nasprotujeta. 19. člen namreč npr. za vodenje seznama kontaktov pooblašča pristojni nacionalni organ (domnevamo, da gre za organ po 21. členu predloga zakona) ter določa da posamezni CSIRT-i posedujejo le kopije kontaktnih podatkov, za katere so pristojni. 23. člen pa v tretji točki drugega odstavka določa, da sezname na podlagi 19. člena predloga zakona vodi vladni CSIRT. Z vidika zagotavljanja točnosti in ažurnosti podatkov ter pravne varnosti glede tega, kateri organ je odgovoren za posamezne vidike izvrševanja nalog upravljavca (lahko gre tudi za soupravljanje posameznih evidenc in delitev nalog), predlagamo, da navedene nejasnosti v besedilu popravite.

Dodatno se pripomba redakcijske narave nanaša na poimenovanja našega organa v 5. točki 21. člena ter v 27. členu, kjer mora pisati Informacijski pooblaščenec (z veliko začetnico), saj gre na tem mestu za poimenovanje organa in ne osebe.

S spoštovanjem,

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

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