INFORMACIJSKI POOBLAŠČENEC
Zaloška 59, 1000 Ljubljana, Slovenija
Telefon: 01 230 97 30
Faks: 01 230 97 78
E-pošta: gp.ip@ip-rs.si
www.ip-rs.si
REPUBLIKA SLOVENIJA

Zadeva: 0712-1/2016/574
Datum: 9. 3. 2016

Direktorat za informatiko
Ministrstvo za javno upravo

Zadeva: Mnenje glede osnutka Uredbe o informacijski varnosti

Spoštovani,

Informacijski pooblaščenec (v nadaljevanju IP) je prejel vaše sporočilo dopis, v katerem nas prosite za mnenje glede osnutka Uredbe o informacijski varnosti (verzija 2.15)

Avtentično razlago posameznih določb zakona daje le Državni zbor, neobvezno pa predlagatelj zakona, zato vam na podlagi informacij, ki ste nam jih posredovali, v nadaljevanju na podlagi 7. točke 1. odstavka 49. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1) ter 2. člena Zakona o informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, v nadaljevanju ZInfP), posredujemo naše neobvezno mnenje v zvezi z vašim vprašanjem.

Informacijski pooblaščenec uvodoma pozdravlja napore in trud, ki ste jih vložili v pripravo osnutka uredbe o informacijski varnosti ter dejstvo, da ste v pripravi uredbe upoštevali nekatera od naših priporočil, ki smo jih podali v mnenju št. 0712-1/2015/3152, z dne 28. 12. 2015 (na verzijo 2.7), zato se v tokratnem mnenju osredotočamo le na tiste določbe, ki so po našem mnenju še potrebne sprememb oziroma prilagoditev.

K 34. členu

V 4. odstavku 34. člena ste glede na naša priporočila zapisali določbe o uporabi informacijsko-tehnološke opreme organa, in sicer:

> *(4) Pred prekinitvijo delovnega razmerja je uslužbenec organa dolžan izbrisati vse zasebne podatke in zasebno korespondenco z informacijsko-tehnološke opreme organa, ki mu je bila dodeljena v uporabo. Organ mora uslužbencu omogočiti, da si pred brisanjem zasebne podatke in zasebno korespondenco kopira na lastne nosilce podatkov. O brisanju in kopiranju se pripravi zapisnik, ki ga podpišeta uslužbenec in pristojna oseba organa.*

Menimo, da je navedeno določbo potrebno izboljšati, termin »zasebni podatki« bi namreč povzročal težave glede interpretacije, kaj vse naj bi ti podatki zajemali v relaciji do termina »osebni podatki«, zato predlagamo, da izraz »zasebne podatke zamenjate s »podatke zasebne narave[1]««.

K 40./56. členu

[1] Gre za podatke oziroma tudi datoteke zasebne narave, ki jih zaposleni hranijo na službenih napravah, kot so slike, besedilni dokumenti, video zapis, preglednice in druge datoteke, ki lahko (ne pa nujno) vsebujejo njihove osebne podatke ali pa so zgolj zasebne narave, pa tudi podatki, ki nastajajo ob njihovi uporabi npr. interneta (zgodovina obiskanih spletnih strani, nameščeni piškotki ipd.).

Kot smo opozorili v prejšnjem mnenju, odsotnost roka hrambe podatkov o uporabi interneta vodi v zelo različno ureditev tega področja pri državnih organih in v primere nenamenske uporabe teh podatkov, kar predstavlja kršitev ZVOP-1, zato menimo, da je koristno določiti rok hrambe teh podatkov, ki naj upošteva zakonite in legitimne namene uporabe teh podatkov. Vendar pa ob tem menimo, da bi določitev roka morala biti izvedena le v tem členu, saj določitev splošnega roka hrambe v 56. členu (dnevniški zapisi) prinaša dodatne težave, saj ni primerno enako obravnavati dnevniških zapisov, ki obenem predstavljajo izpolnjevanje zahtev glede sledljivosti obdelave osebnih podatkov in vseh ostalih dnevniških zapisov.

V informacijskem sistemu namreč obstajajo številni dnevniški zapisi – nekateri od njih (ne pa vsi) obenem predstavljajo dnevniške zapise, ki po vsebini ustrezajo zahtevam po sledljivosti obdelave osebnih podatkov (predvsem beleženje dostopa do osebnih podatkov v zbirkah osebnih podatkov) po 24. členu ZVOP-1, za katere pa je zakonsko zahtevani rok hrambe 6 let; več o tem glej Smernice o zavarovanju, dostopno na:
https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf

Določitev krajšega roka hrambe v uredbi (»hramba dnevniških zapisov, ki vsebujejo osebne podatke«, predlagani 5. odstavek 56. člena predloga uredbe) bi bila zato v delu, kjer dnevniški zapisi hkrati predstavljajo zapise sledljivosti obdelave osebnih podatkov, v neposrednem nasprotju z določbami ZVOP-1. Podobno težavna je lahko določitev roka hrambe glede beleženja fizičnih dostopov v varovana območja organa (v primerih, ko gre za isto evidenco, kot je evidenca vstopov in izstopov z oz. iz prostorov), saj to evidenco ureja 82. člen ZVOP-1, ki določa:

> *(1) Oseba javnega ali zasebnega sektorja lahko za namene varovanja premoženja, življenja ali telesa posameznikov ter reda v njenih prostorih od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi lahko osebne podatke preveri tudi z vpogledom v osebni dokument posameznika.*
> *(2) V evidenci vstopov in izstopov se lahko o posamezniku vodijo samo naslednji osebni podatki: osebno ime, številka in vrsta osebnega dokumenta, naslov stalnega ali začasnega prebivališča, zaposlitev ter datum, ura in razlog vstopa ali izstopa v ali iz prostorov.*
> *(3) Evidenca iz prejšnjega odstavka velja za uradno evidenco v skladu z zakonom, ki ureja splošni upravni postopek, če je potrebno pridobiti podatke z vidika koristi mladoletnika ali za izvrševanje pristojnosti policije ter obveščevalno-varnostne dejavnosti.*
> *(4) Osebni podatki iz evidence iz drugega odstavka tega člena se lahko hranijo največ tri leta od vpisa, nato se zbrišejo ali na drug način uničijo, če zakon ne določa drugače.*

Prav tako se nam zdi generalna določitev roka hrambe za vse, zelo raznolike, dnevniške zapise na splošno problematična zaradi različnih okoliščin in s tem namenov uporabe in je vsaj v nekaterih primerih v nasprotju z določbami ZVOP-1, zato predlagamo, da se brišeta 5. in 6. odstavek 56. člena predloga uredba.

Podatki o uporabi interneta s strani zaposlenih[2] pa ne predstavljajo sledljivosti po 24. členu ZVOP-1, zato v tem delu predlagamo določitev hrambe, ki pa naj bo opredeljena v 40. členu, ki ureja uporabo interneta – predlagamo skratka, da določbo 5. odstavka 56. člena premaknete v 40. člen, pri čemer jo seveda smiselno prilagodite, da se bo nanašala zgolj na hrambo podatkov o uporabi interneta. Kot smo že zapisali v prvem mnenju, upoštevajoč načelo sorazmernosti predlagamo, da se ti podatki hranijo 30 dni[3].

[2] Kdo je dostopal do podatkov o uporabi interneta po uporabniku predstavlja podatke o sledljivosti po 24. členu ZVOP-1.
[3] Najdaljši rok, ki se nam še zdi sprejemljiv, je tri mesece.

Če bi potrebovali dodatna pojasnila, smo vam na voljo.

S prijaznimi pozdravi,

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

Pripravil:

- mag. Andrej Tomšič, namestnik informacijske pooblaščenke