

Številka:
Datum: 23.1.2009

**Ministrstvo za gospodarstvo
Direktorat za elektronske komunikacije
Kotnikova 5**

1000 Ljubljana

Zadeva: Stališče Informacijskega pooblaščenca glede predloga Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-B)

Spoštovani!

Na podlagi 1. odstavka 48. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1) vam posredujemo stališče Informacijskega pooblaščenca (v nadaljevanju: Pooblaščenec) z vidika njegovih pristojnosti glede ustavno zagotovljenega varstva osebnih podatkov glede predlaganih sprememb Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-B), ki so bile objavljene na spletnih straneh Ministrstva za gospodarstvo.

Pooblaščenec v zvezi s tem uvodoma pozdravlja dejstvo, da je predlagatelj zakona v predlaganih rešitvah sprejel že poslano predloge Informacijskega pooblaščenca, ki se nanašajo na posredovanje prometnih podatkov v primerih varovanja življenja in telesa (104.a člen), nadzor (112. člen) in sankcioniranje v tem oziru (45.a in 45.b člen). Predlagamo pa, da se v 104.a členu izbriše možnost usnega podajanja zahtev za posredovanje podatkov. S tem se po naših informacijah strinjata tako policija kot tudi operaterji.

Ob tem pa Pooblaščenec predlaga, da se predlagani 45.a člen glasi:

»45.a ne hrani dokumentacije, ugotovitev ali zahtev oziroma podatkov na način in pod pogoji iz 107.c člena zakona ali ne zagotavlja neizbrisne registracije izvedenih ukrepov in posegov v skladu s 107.č členom tega zakona (tretji odstavek 104.a člena)«.

Glede ostalih predlaganih sprememb, ki se nanašajo na posredovanje prometnih podatkov v primerih varovanja življenja in telesa, Pooblaščenec nima pripomb.

Kar se tiče predlaganih sprememb 107. b člena Pooblaščenec pozdravlja odpravo redakcijske napake ter spremembo glede podrobnejše ureditve hrambe podatkov v podzakonskem aktu, ki jo uvaja novi odstavek 107. c člena.

Pripombe, ki se nanašajo na nov sedmi odstavek 91. člena (razčlenjeni račun)

12. člen ZEKom-B predvideva naslednjo spremembo 91. člena ZEKom:

»(7) Če operater nudi tudi takšno stopnjo razčlenitve računa, pri kateri je mogoče razpoznati identiteto klicanih oseb, mora operater, če uporabnik tako zahteva, temu omogočiti račun, ki je razčlenjen tako, da druge osebe ne morejo razpoznati identitete klicanih oseb (na primer z zakritjem dela števil klicanih oseb).«

Pooblaščenec je mnenja, da je potrebno predlagano določbo razširiti tudi na identiteto kličočih, saj se v nekaterih primerih lahko tudi prejeti klici zaračunajo (ko je npr. klicana oseba v tujini), posledično pa se lahko tudi podatki o kličočem pridobijo na razčlenjenem računu.

V zvezi z uporabo podatkov iz razčlenjenega računa je potrebno glede na odločbo Upravnega sodišča RS št. U702/99-48 zagovarjati stališče, da se podatki iz razčlenjenega računa lahko uporabljajo le za kontrolo obračunavanja in plačevanja telefonskih storitev, vsaka drugačna uporaba takšnih podatkov pa lahko pomeni kršitev 8. ali 16. člena ZVOP-1. Razčlenjeni obračun je sicer omenjen v 33. točki in v 7. členu Direktive o

zasebnosti in elektronskih komunikacijah 2002/58/ES. Iz 33. točke Direktive 2002/58/ES izhaja, da lahko države članice zaradi ohranitve zasebnosti določijo, da se naročnikom posreduje račun, na katerem je izbrisano določeno število števil klicane osebe. Pooblaščenec tako pozdravlja predlog sprememb 91. člena ZEKom, ki omogoča anonimizacijo telefonskih števil na razčlenjenem računu, vendar meni, da je potrebno predlagano določbo spremeniti predvsem v luči nenamenske uporabe podatkov na razčlenjenem računu s strani delodajalcev. Glede na namen razčlenjenega računa, t.j. preverjanje pravilnosti obračuna storitev, je torej potrebno poiskati rešitev, ki ne ovira izpolnitve tega namena, obenem pa zagotavlja varovanje informacijske zasebnosti posameznikov. Informacijski pooblaščenec predlaga, da se zakritje dela števil uvede **kot pravilo ter da se določi, v katerih primerih so možne izjeme od tega pravila**. Med izjeme lahko sodi primer, ko ima podjetje sklenjena naročniška razmerja za več zaporednih telefonskih števil (t.i. poslovna omrežja). V takšnem primeru so lahko tudi klici znotraj takšnega poslovnega omrežja zaračunajo, zakritje zadnjih nekaj števil pa bi naročniku preprečilo, da lahko preveri pravilnost obračuna. Prav tako bi zakrivanje zadnjih nekaj števil pri tistih naročnikih, ki so fizične osebe, verjetno povzročilo precejšnje nerazumevanje, zato je predvidena izjema tudi za fizične osebe, ki izrecno izrazijo zahtevo, da operater ne anonimizira prometnih podatkov. Ključno je, da se prepreči zlorabe podatkov o klicih v delovnem okolju, t.j. da bi delodajalec na podlagi podatkov o klicih izvajal nadzor nad zaposlenimi, kar je v nasprotju s 16. členom ZVOP-1, ki določa, da se lahko osebni podatki uporabljajo samo za namen, za katerega so bili zbrani, pri razčlenjenem računu pa je ta namen izključno preverjanje veljavnosti obračuna storitev.

Pooblaščenec na podlagi navedenega predlaga naslednje besedilo novega sedmega odstavka 91. člena:

»(7) Če operater nudi tudi takšno stopnjo razčlenitve računa, pri kateri je mogoče razpoznati identiteto klicanih ali kličočih oseb, mora operater uporabniku omogočiti račun, ki je razčlenjen tako, da druge osebe ne morejo razpoznati identiteto klicanih ali kličočih oseb z zakritjem dela števil klicanih ali kličočih oseb. Zakritja dela števil klicanih ali kličočih oseb ni potrebno zagotavljati za klice med internimi številkami istega naročnika ali na podlagi zahteve naročnika, ki v razmerju do operaterja nastopa kot fizična oseba.«

Pooblaščenec prav tako poziva predlagatelja zakona, da **čim prej popravi Splošni akt o razčlenjenem računu** iz leta 2002, ki je bil sprejet še na podlagi Zakona o telekomunikacijah (ZTel-1). Številni operaterji namreč ponujajo vpogled v sezname dohodnih in odhodnih ter zgrešenih klicev prek servisnih spletnih strani, pri čemer se nekateri operaterji odločajo za anonimizacijo števil, drugi pa ne, zato je Pooblaščenec mnenja, da je potrebno tovrstno dostopnost podatkov o klicih (in druga vprašanja, ki se nanašajo na razčlenjen račun), podrobneje in enovito urediti v novem splošnem aktu, pri tem pa upoštevati zgoraj navedeni predlog ureditve.

Pripombe, ki se nanašajo na četrti odstavek 107.a člen (obvezna hramba podatkov)

Pooblaščenec predlaga spremembo četrtega odstavka 107.a člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 13/2007 - uradno prečiščeno besedilo, ZEKom-UPB1), ki ureja **rok hrambe podatkov iz 107.b člena ZEKom**. Po primerjalnem pregledu stanja po drugih državah, je trenutni rok hrambe predolg, saj so se vse države z izjemo Italije in Irske odločile za krajši rok hrambe, kot ga dopušča Direktiva 2006/24/ES (Uradni list L 105, 13/04/2006 str. 0054 – 0063; v nadaljevanju direktiva). Po podatkih, ki jih je uspel pridobiti Pooblaščenec, so namreč roki hrambe po državah članicah naslednji:

Avstrija – 6 mesecev (predlog)

Belgija – direktiva še ni prenešena v nacionalno zakonodajo

Bolgarija – 12 mesecev¹

Češka – 12 mesecev

Ciper – 6 mesecev

Danska – 12 mesecev

Estonija – 12 mesecev **Finska** – n.p.

Francija – 12 mesecev

Nemčija – 6 mesecev

Grčija – 12 mesecev

Madžarska – n.p.

Irska² – 3 leta

Italija – 2 leti za mobilne telekomunikacije, 6 mesecev za internet, 4 leta za telefonijo

¹ Bolgarsko Vrhovno sodišče (Bulgarian Supreme Administrative Court (SAC)) je 11. decembra 2008 razveljavilo določila o obvezni hrambi prometnih podatkov v Bolgariji.

² Irska direktivo o obvezni hrambi podatkov izpodbija na Sodišču evropskih skupnosti v Luksemburgu.

Latvija – 18 mesecev
Litva – n.p.
Luksemburg – 6 mesecev
Malta – n.p.
Nizozemska – 3 mesece za predplačniške mobilne telefone (splošen predlog 1 leto)
Poljska – n.p.
Portugalska – direktiva še ni prenešana v nacionalno zakonodajo
Romunija – 6 mesecev
Slovaška – 6 mesecev za internet, 24 mesecev za druge oblike komunikacije
Španija – 12 mesecev
Švedska – 12 mesecev
Velika Britanija – 12 mesecev³

Informacijski pooblaščenec je mnenja, da dolgotrajnost in manjša učinkovitost izvajanja predkazenskih in kazenskih postopkov ni argument, ki bi upravičeval daljši rok hrambe, kot si ga je izbrala večina držav članic EU. Ne gre zanemariti tudi stroškovne vidike tako dolgega roka hrambe podatkov, ki jih morajo nositi operaterji, ki za to niso kompenzirani s strani države in so tako posredno prisiljeni financirati slabšo učinkovitost organov pregona. Daljši rok hrambe predstavlja večje možnosti za zlorabe in s tem nezakonite posege v zasebnost posameznikov. Ob upoštevanju dejstva, da so stroški, potrebni za zagotovitev resnično varnih rešitev za shranjevanje podatkov, za operaterje vsekakor visoki, obstaja še večja teža na možnostih za zlorabe, če se operaterji odločijo za cenejše in manj varne rešitve. V Veliki Britaniji tako ocenjujejo, da je investiranje v varne in učinkovite rešitve za hrambo podatkov ključno za učinkovitost zakonodaje, ki takšno hrambo predpisuje, in bodo kompenzirali stroške, ki jih bodo imeli operaterji z vlaganji v nabavo, delovanje in vzdrževanje rešitev za hrambo podatkov⁴. Rok hrambe je tako z vidika sorazmernosti, možnih zlorab in stroškov eden izmed odločilnih faktorjev, zato je zelo pomembno, da rok hrambe ni prekomeren. Za skrajšanje roka hrambe so se na podlagi analiz o sorazmernosti roka hrambe odločili tudi na Nizozemskem⁵.

Informacijski pooblaščenec se v odnosu do direktive pridružuje svojim kolegom, t.j. organom za varstvo osebnih podatkov držav EU iz kroga neodvisnega evropskega svetovalnega organa za varstvo osebnih podatkov in zasebnosti, t.i. Article 29 Data Protection Working Party ter Evropskemu nadzorniku za varstvo osebnih podatkov (European Data Protection Supervisor - EDPS). Omenjeni organi so večkrat izrazili zaskrbljenost ob sprejemanju Direktive, tako je Article 29 Data Protection Working Party dne 21.10.2005 sprejel *Mnenje evropskih organov za varstvo osebnih podatkov (Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005) 438 final of 21.09.2005)*. Mnenje je dosegljivo na naslovu:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_sl.pdf

Informacijski pooblaščenec je mnenja, da ostajajo stališča, ki so zastopana v navedenem mnenju, z zornega kota osnovnih načel varstva zasebnosti in osebnih podatkov veljavna in utemeljena, kljub temu, da so bila pripravljena v času, ko direktiva še ni bila uradno sprejeta. Med ključne poudarke za zaskrbljenost organov za varstvo osebnih podatkov v zvezi z direktivo med drugim sodijo naslednji:

- Vsaka omejitev temeljne pravice zaupnih komunikacij mora temeljiti na nujni potrebi, dovoljena mora biti le v izjemnih primerih in biti predmet ustreznih zaščitnih ukrepov.
- Ukrepi za boj proti terorizmu morajo biti zasnovani tako, da se učinkovito zadovoljijo potrebe svojih državljanov po življenju v miru in varnosti, ne da bi bile pri tem njihove individualne človekove pravice, vključno s pravico do zasebnosti podatkov, ki predstavljajo temelj naše demokratične družbe, ogrožene.
- Vprašanje sorazmernosti obdelave osebnih podatkov v okviru ukrepov, ki jih uvaja Direktiva z vidika število obravnavanih posameznikov in obdobja hrambe glede na prvotni namen zbiranja podatkov.
- Redno ocenjevanje ukrepov, ki jih uvaja Direktiva v luči doseganja zelenih učinkov.

³ Podatki o naročnikih in telefonskih klicih - 12 mesecev, SMS, EMS in MMS - 6 mesecev, e-pošta – 6 mesecev, podatki o dostopu do interneta – 6 mesecev, dnevniki o spletnih aktivnostih – 4 dni.

⁴ Stroški operaterjev naj bi znašali med 25 in 70 milijoni funtov (http://news.bbc.co.uk/2/hi/uk_news/7819230.stm).

⁵ <http://www.edri.org/edriagram/number6.11/nl-data-retention-12-months>.

- Vprašanja varnosti podatkov, dostopa tretjih oseb do podatkov, nadzora, obveščanja javnosti in drugih elementov varstva osebnih podatkov, kot izhaja iz mnenja Article 29 Data Protection Working Party.

Ob upoštevanju načela sorazmernosti, kot temeljnega načela varstva osebnih podatkov, in na podlagi navedenega Informacijski pooblaščenec predlaga, da se rok hrambe v četrtem odstavku 107.a člena ZEKom skrajša na **6 mesecev** oziroma na največ 12 mesecev.

Kar se tiče predlaganih sprememb 107.b člena Pooblaščenec pozdravlja odpravo redakcijske napake ter spremembo glede podrobnejše ureditve hrambe podatkov v podzakonskem aktu, ki jo uvaja novi odstavek 107. c člena.

Pripombe, ki se nanašajo na četrty odstavek 107.č člena (hramba posredovanih podatkov)

Četrty odstavek 107.č člena med drugim določa, da **morajo operaterji pridobljene in izročene podatke hraniti trajno**, kar je po mnenju Pooblaščenca neprimerno in absolutno predolgo.

Direktiva v 7d členu ne določa, da je potrebno pridobljene in izročene podatke hraniti trajno, temveč določa, da: *»ob koncu obdobja hranjenja se uničijo vsi podatki, razen tistih, do katerih se je dostopalo in se jih shranilo.«* Direktiva torej **ne zahteva trajnosti hrambe teh podatkov**, obenem pa tudi **ne predpisuje roka hrambe**. Glede na namen uporabe teh podatkov glede na določbe prvega odstavka 107.b člena, je pooblaščenec mnenja, da je potrebno roke hrambe urediti skladno z nameni uporabe podatkov.

Roke hrambe osebnih podatkov, med katere gotovo sodijo tudi podatki, ki se hranijo na podlagi 107.b člena ZEKom, na sistemski ravni ureja **21. člen Zakona o varstvu osebnih podatkov** (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1), ki določa, da se **osebni podatki lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali**. Drugi odstavek 21. člena dalje določa, da se po izpolnitvi namena obdelave osebni podatki zbirajo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Deveto poglavje Kazenskega zakonika (Ur. l. RS, št. 55/2008 s spremembami in dopolnitvami; v nadaljevanju KZ) opredeljuje rehabilitacijo, izbris obsodbe in pogoje za dajanje podatkov iz kazenske evidence in med drugim v 3. odstavku 82. členu določa, da se obsodba izbriše iz kazenske evidence v določenem roku, od takrat ko je bila kazen izvršena, zastarana ali odpuščena, če obsojenec v tem roku ne stori novega kaznivega dejanja.

4. odstavek 82. člena določa roke za izbris:

- 1) za obsodbo, s katero je bil storilcu izrečen sodni opomin, in za obsodbo, s katero mu je bila odpuščena kazen – eno leto od pravomočnosti sodne odločbe;
- 2) za pogojno obsodbo – eno leto, od takrat ko je potekla preizkusna doba;
- 3) za obsodbo na denarno kazen, stransko kazen ali kazen zapora do enega leta – tri leta;
- 4) za obsodbo na kazen zapora nad eno leto do treh let – pet let;
- 5) za obsodbo na kazen zapora nad tri leta do petih let – osem let;
- 6) za obsodbo na kazen zapora nad pet do deset let – deset let;
- 7) za obsodbo na kazen zapora nad deset do petnajst let – petnajst let.

Trajna hramba pridobljenih in izročenih podatkov bi lahko privedla do situacije, v kateri bi se podatki o posamezniku, ki je bil na podlagi tako pridobljenih podatkov bodisi oproščen bodisi pravomočno obsojen in ki je že prestal odrejeno kazen, kljub temu še vedno hranili pri operaterju. Pooblaščenec je mnenja, da ne obstajajo razlogi, ki bi utemeljevali trajno hrambo dejansko posredovanih podatkov, zato predlaga, da za te podatke določimo 5 letni rok hrambe, ki ustreza definiciji iz 21. člena ZVOP-1. Ta rok je v skladu z načelom sorazmernosti primeren glede na določila Obligacijskega zakonika, ki določajo kot absolutni 5 letni rok za sprožitev ustreznih civilnopravnih in odškodninskih sporov. To velja tudi za kršitev osebnostnih pravic, kamor civilnopravno gledano sodi tudi varstvo osebnih podatkov. Takšen rok ustreza tudi določilu 22. člena ZVOP-1, ki nalaga obveznost upravljavcem zbirk osebnih podatkov v zvezi s t.i. zunanjo sledljivostjo uporabe posameznih osebnih podatkov.

Pooblaščenec zato predlaga, da se **četrty odstavek 107.č člena spremeni tako, da se glasi:**

»(4) Operaterji morajo skupaj s pristojnimi organi, ki lahko zahtevajo dostop do hranjenih podatkov, zagotoviti neizbrisno registracijo vseh posredovanj hranjenih podatkov. Pridobljene in izročene podatke operaterji **hranijo 5 let po posredovanju podatkov** ter jih varujejo v skladu z oznako stopnje tajnosti prepisa odredbe.«
Za konec pa v razmislek podajamo še en predlog, ki je vezan na obdelavo osebnih podatkov in neposredno trženje.

Morda bi kazalo premisliti o tem, da se posameznikom, katerih osebni podatki so objavljeni v javnem telefonskem imeniku, da možnost prepovedati uporabo objavljenih podatkov za namene neposrednega trženja, anketiranja in politične propagande. V ta namen bi bila potrebna dopolnitev 110. in 111. člena ZEKom, in sicer tako, da se da naročnikom možnost, da se v imeniku vodi tudi podatek o tem, da naročnik ne dovoljuje uporabe svojih osebnih podatkov za prej navedene namene neposrednega trženja, uporaba tako označenih podatkov za namene neposrednega trženja pa bi morala biti seveda tudi ustrezno sankcionirana.

S takšno dopolnitvijo zakona bi ugodili tistim naročnikom, ki sicer želijo objavo svojih podatkov v javnem telefonskem imeniku, vendar pa podatkov ne objavijo ravno iz razloga, ki ne želijo prejemati propagandnih klicev.

Posameznikom, ki ne dovolijo uporabe svojih osebnih podatkov za namene neposrednega trženja, bi s takšno ureditvijo dali možnost, da takšno svojo voljo izrazijo le enkrat – izdajatelju imenika, sedaj pa morajo to svojo pravico uveljavljati pri vsakem upravljavcu, izvajalcu neposrednega trženja, anketarju itd. posebej.

Z zgoraj navedeno dopolnitvijo bi tudi v Sloveniji dobili neke vrste »*Do not call register*«.

Če bi sprejeli zgoraj predlagano ureditev, bi se lahko za namene neposrednega trženja uporabljali le še tisti osebni podatki, ki jih je posamezni upravljavec zbral v okviru zakonitega opravljanja dejavnosti, poleg tega pa bi imeli upravljavci tudi možnost, da na podlagi osebne privolitve posameznika vzpostavijo posebne zbirke, ki so namenjene predvsem za izvajanje neposrednega trženja.

Predlagamo, da navedene pripombe upoštevate in se vam obenem ponovno zahvaljujemo za trud in prizadevanje, ki ste ga in ga še boste vložili v rešitev oziroma izboljšavo predloga zakona.

S spoštovanjem,

Informacijski pooblaščenec:
Nataša Pirc Musar, univ.dipl.prav.,
pooblaščenka

Vročiti:

- Naslovniku navadno in po elektronski pošti na gp.mg@gov.si
- Arhiv, tu.

V vednost:

- Agencija RS za pošto in elektronske komunikacije – info.box@apek.si
- Ministrstvo za zunanje zadeve – gp.mzz@gov.si