INFORMACIJSKI POOBLAŠČENEC
Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Telefon: + 386 (0) 1 230 97 30
Faks: + 386 (0) 1 230 97 78
www.ip-rs.si
REPUBLIKA SLOVENIJA

Datum:
Številka: 007-21/2011/

Direktorat za informacijsko družbo
Ministrstvo za izobraževanje, znanost, kulturo in šport
Masarykova cesta 16, 1000 LJUBLJANA

e-naslov: gp.mizks@gov.si

Zadeva: Odgovor Informacijskega pooblaščenca glede povratne informacije o upoštevanju pripomb in predlogov, posredovanih na predlog Zakona elektronskih komunikacijah (ZEKom-1) - EVA 2012-3330-0058
Zveza: Vaš dopis št. 0070-56/2012/58 z dne 1.8.2012 in gradivo

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) je Informacijski pooblaščenec (v nadaljevanju: Pooblaščenec) na predlog Zakona o elektronskih komunikacijah (v nadaljevanju: predlog ZEKom-1) že podal pripombe 2. in 3. 7. 2012. Z zgoraj navedenim dopisom ste nam posredovali povratno informacijo o vključitvi naših pripomb v predlog ZEKom-1.

Za povratno informacijo in sprejem nekaterih pripomb se vam zahvaljujemo, hkrati pa glede na vaše argumente o (ne)sprejemljivosti določenih naših pripomb in naknadne ugotovitve dodajamo, kot sledi.

K 149. členu
Definicija elementov oštevilčenje je sedaj bolj natančna in številke internetnega protokola (IP) ne sodijo med elemente oštevilčenje. Tako se pojavi vprašanje smiselnosti navedenih določb - ob dejstvu, da so organi, ki vodijo inšpekcijski, predkazenski ali sodni postopek pooblaščeni za pridobitev in nadaljnjo obdelavo osebnih podatkov po postopkovnih zakonih (torej po zakonu o inšpekcijskem nadzoru, zakonu o kazenskem postopku, zakonu o pravdnem postopku ipd.). Določbe prvega in drugega odstavka 149. člena so bile vnesene v enega prvih predlogov za spremembo ZEKom, ko se je še razmišljalo o hrambi IP številk med podatki o naročnikih. Potem, ko smo skupaj ugotovili, da takšna rešitev ni primerna, so postale te določbe nesmiselne (nepotrebne). Kot take pa lahko med naslovniki ustvarjajo zmedo o tem, kakšno novo pooblastilo prinašajo in v kakšnih primerih se uporabi in ne prispevajo k preglednosti zakona. Morda bo celo ustvarila vtis, da so operaterji organom dolžni posredovati le te (ozko navedene) podatke, kar pa ne drži, ker je treba upoštevati specialne podlage iz postopkovnih in področnih zakonov.

Zaradi navedenega predlagamo, da se celoten 149. člen predloga ZEKom-1 izpustiti.

Poudarjamo, da po našem vedenju v tem primeru ni šlo za implementacijo določbe 15a člena Direktive 136/2009, ki določa, da imajo pristojni nacionalni organi in po potrebi drugi nacionalni organi potrebna preiskovalna pooblastila in sredstva, vključno s pooblastilom za pridobitev vseh ustreznih informacij, ki so potrebne za spremljanje in izvrševanje nacionalnih določb, sprejetih na podlagi te direktive.

Nacionalni organi v Republiki Sloveniji že imajo ustrezna pooblastila za opravljanje svojih nalog, ki jih ZEKom (skladno z Ustavo RS) omejuje – kot gre za t.i. prometne podatke, ki se hranijo. Največjo operativno težavo pri delu preiskovalnih organov pri nas predstavlja dostop do vsebine komunikacije in z njo povezanimi podatki. Ker pa tega problema, brez spremembe Ustave RS ali vsaj novega tolmačenja ustavnega sodišča z ZEKom ni mogoče rešiti, so citirane določbe povsem odveč in bi le ustvarjale zmedo o vsebini in obsegu pristojnosti inšpekcijskih, prekrškovnih in sodnih organov.

Tretji odstavek, ki določa roke hrambe podatkov o zahtevah organov pri operaterju, tudi ni potreben, saj že ZVOP-1 določa, da mora vsak upravljavec osebnih podatkov (torej tudi operater) hraniti podatke o tem, komu, na kakšni pravni podlagi, za kašnem namen, kdaj in katere osebne podatke o posamezniku je posredoval – za obdobje, ko je dopustno izpodbijati obdelavo zaradi domnevne zlorabe osebnih podatkov (22. člen in 30. člen ZVOP-1).

Kot že navedeno predlagamo, da se celoten člen izpusti. Ob zgoraj navedenih argumentih za nesmiselnost prvega, drugega in tretjega odstavka je očitno, da tudi četrti odstavek, ki določa nadzor informacijskega pooblaščenca nad ravnanjem po tem členu, nima nobene dodane vrednosti. Informacijski pooblaščenec bo nadzor pač opravljal po ZVOP-1, saj je vsa materija, ki jo ureja 149. Člen že urejena v področnih zakonih, ki urejajo položaj pristojnih organov – ta člen bi jih uredil v nasprotju s področnimi zakoni. Seveda bi bilo v tem primeru treba izpustiti tudi sklice na ta člen (v 148. členu, v 151. členu in v 155. členu).

K 151. členu
(prvi odstavek)
Še vedno menimo (kljub vašim argumentom v povratni informaciji), da so roki hrambe podatkov v prvem odstavku 151. člena določeni nejasno in lahko v praksi pripeljejo do prekomerne hrambe – ko bi operaterji razumeli, da morajo vselej (za vsak slučaj) hraniti podatke dlje kot je to potrebno za prenos sporočil. To seveda ne drži. Operater hrani podatke dlje, le če so bili podatki neposredno povezani s specifično situacijo, za katero ZEKom odreja drugače režim 8tudi drugačen rok hrambe).

Predlagamo, da se prvi odstavek 151. člena predloga ZEKom-1 spremeni, tako da se glasi:
»Podatki o prometu, ki se nanašajo na naročnike in uporabnike ter jih je operater obdelal in shranil, morajo biti izbrisani ali spremenjeni tako, da se ne dajo povezati z določeno ali določljivo osebo takoj, ko niso več potrebni za prenos sporočil, razen v primerih podatkov, pri katerih je po tem zakonu določen daljši rok hrambe; glede zakonitega prestrezanja (160. člen), glede posredovanja prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa (153. člen) in glede njihovih obveznosti, ki izhajajo iz poglavja o hrambi podatkov tega zakona (162., 163., 164., 165., 166., 167. in 168. člen).«

(drugi odstavek)
Pooblaščenec ponavlja pripombo, in vztraja, da je novi odstavek manj pregleden in določen od veljavne določbe, ki glasi: Ne glede na določbo prejšnjega odstavka lahko operater **do popolnega plačila storitve**, vendar najdlje do preteka zastaralnega roka, hrani in obdeluje podatke o prometu, ki jih potrebuje za obračun in za plačila v zvezi z medomrežnim povezovanjem.

Dejstvo je, da mora imeti operater na razpolago podatke do popolnega poplačila, vendar najdlje do poteka zastaralnega roka. Ob novi dikciji določbe se tako postavlja vprašanje, koliko časa bodo operaterji hranili podatke o tistih naročnikih, ki bodo terjatev v celoti poplačali v roku (kar stori velika večina naročnikov). Hraniti tudi v teh primerih podatke celo leto, bi bilo prekomerno, saj med strankama (operaterjem in naročnikom) plačilo ni sporno. Poleg tega dostavek v novem predlogu, ki pravi: …*še največ za obdobje enoletnega zastaralnega roka za svoje terjatve za izvajanje storitev*

skladno z zakonikom, ki ureja obligacijska razmerja, lahko tudi zavaja operaterje. Če bi operater moral npr. prisilno izterjati terjatev, bi lahko postopek izvršbe trajal dlje, zastaranje bi bilo pretrgano, slovnična razlaga določbe pa mu nalaga uničenje podatkov po poteku enoletnega zastaralnega zakona.

Predlagamo torej, da se določba drugega odstavka nadomesti z zdaj veljavno.

K 155. členu (tretji odstavek)

Člen ureja sledenje zlonamernih klicev in tudi možnost prizadetega, da izve za identiteto klicatelja. Pripomba Pooblaščenca, ki jo je podal 2.7.2012 na to določilo, ni bila sprejeta. Argumente, ki ste jih navedli, sprejemamo, še vedno pa menimo, da mora biti popolnoma jasno, kdaj bo naročnik – prizadeti upravičen do identifikacijskih podatkov zlonamernega klicatelja.

Tako predlagamo, da se tretji odstavek spremeni, tako da glasi: Identiteto kličočega operater razkrije naročniku, ki izkaže pravni interes za zaščito svojih pravic pred sodiščem.

Namesto »najave tožbe« naj naročnik zatrjuje obstoj pravnega interesa za pridobitev podatka. Če bi določilo tretjega odstavka spremenili, kot predlagamo, bi šlo za podobno možnost, kot jo v drugem odstavku pozna 22. člen ZVOP-1. Žal se v tem primeru (tudi, če ostane zapisano, da posameznik »najavi tožbo«) ne bo mogoče izogniti presoji o prizadetosti naročnika s strani operaterja. Zadeva ne bo problematična, kadar bo šlo za ekstremne situacije številnih klicev v relativno kratkem obdobju na naročnikovo številko. Težave pa lahko nastanejo v primeru, ko bi naročniki trdil, da je bil določen (en sam) klic zlonameren in zato želi identiteto klicatelja. Ker je naslov člena določen v množini »sledenje zlonamernih ali nadležnih klicev« menimo, da mora biti takšnih klicev resnično več.

K 158. členu

(1. odstavek)

Pooblaščenec poudarja, da po našem vedenju termin »**namen neposrednega trženja«** v nobeni od relevantnih direktiv **ni opredeljen zgolj kot pošiljanje sporočil komercialnega namena**, kakor ste utemeljili ob zavrnitvi našega predloga, da se nameni neposrednega trženja v predlogu ZEKom-1 natančneje opredelijo.

1. odstavek 13. člena Direktive 136/2009 namreč določa zgolj: *Uporaba avtomatičnih klicnih in komunikacijskih sistemov brez človekovega posega (klicni avtomati), faksimilnih naprav (faksov) ali elektronske pošte **za namene neposrednega trženja** je dovoljena samo za naročnike ali uporabnike, ki v to prej privolijo.*

Z vašim argumentom, da Direktiva 136/2009 za neželena sporočila z namenom neposrednega trženja šteje le sporočila komercialnega namena, **se preprosto ne moremo strinjati,** saj ta direktiva **neposrednega trženja nikakor in nikjer ne omeji le na komunikacije komercialnega namena.** Na kontekst komercialne komunikacije do določene mere namiguje le 2. odstavek relevantnega člena, ki govori o »odjemalcu v kontekstu prodaje storitev ali izdelkov«, pri katerem je pravilo vnaprejšnje privolitve omiljeno in je zahtevana le možnost naknadne zavrnitve. Zgolj zaradi te posebne določbe, ki velja v odnosu odjemalec – prodajalec, pa ni mogoče trditi, da je **»namen neposrednega trženja«** zgolj in samo **»komercialni namen v smislu prodaje izdelkov in storitev«.** Vaš argument, da bi z našim predlogom Direktivo netočno prenesli ni na mestu; obratno, z oženjem namena na zgolj komercialni, je tveganje za netočen prenos določbe večji.

O neželenih elektronskih sporočilih govori tudi Direktiva 2000/31/EC, prenesena v ZEPT, ki določa podobne pogoje za pošiljanje komercialnih sporočil (privolitev) in v 2(f) členu jasno določa, da je

„komercialno sporočilo": vsaka oblika sporočila, ***namenjena neposredni ali posredni promociji blaga, storitev ali podobe podjetja, organizacije ali osebe, ki opravlja trgovsko, industrijsko ali obrtno dejavnost ali zakonsko urejeni poklic****. Naslednje samo po sebi še ne predstavlja komercialnega sporočila:*
— podatki, ki omogočajo neposreden dostop do dejavnosti podjetja, organizacije ali osebe, predvsem ime domene ali elektronski naslov,
— sporočila v zvezi z blagom, storitvami ali podobo podjetja, organizacije ali osebe, ki se zagotavljajo neodvisno in brez finančnega nadomestila;

Iz te določbe in določbe prenesene v ZEPT je razvidno, da neželena sporočila oziroma »komercialna« sporočila niso vezana samo na komercialni namen v smislu prodaje izdelkov in storitev, pač pa je to lahko kakršna koli oblika sporočila namenjena neposredni ali posredni promociji. Navedeni izjemi sicer začetno definicijo omilita in izvzameta zgolj povezave na npr. spletno stran in sporočila v zvezi z neodvisnim izvajanjem aktivnosti brez finančnega nadomestila, a je iz dikcije razvidno, da ti izjemi ne veljata absolutno, pač pa je potrebno sporočilo presoditi kot celoto in ugotoviti ali je lahko kljub izjemi opredeljeno kot komercialno sporočilo.

Direktiva 2000/31/EC v 14. uvodni izjavi zelo jasno napotuje na Direktivo 95/46/ES in glede izvajanja pravi: *njeno izvajanje in uporaba bi morala biti popolnoma usklajena z načeli o varstvu osebnih podatkov, predvsem glede nepovabljenih komercialnih sporočil in odgovornosti posrednikov.*

Direktiva 95/46/ES (o varstvu osebnih podatkov) pa v uvodni določbi 30 navaja, da *…lahko države članice prav tako določijo pogoje, pod katerimi se osebni podatki lahko posredujejo tretji stranki v namene trženja, bodisi da se slednje izvaja komercialno ali da ga izvaja dobrodelna organizacija ali katero koli združenje ali ustanova, na primer politične narave, ob upoštevanju določb, ki omogočajo posamezniku, na katerega se osebni podatki nanašajo, da brezplačno in brez navedbe razlogov ugovarja obdelavi podatkov, ki se nanašajo nanj.*

Iz česar je nedvomno razvidno, da neposredno trženje **NI omejeno** na okvir komercialnih komunikacij, pač pa na kakršno koli trženje, torej promocijo, ne glede na to, ali je komercialno in ne glede na entiteto, ki ga izvaja. V skladu z določbami in pojasnili omenjenih Direktiv tako **tržne raziskave**, kjer pošiljatelji zelo pogosto izkoristijo javno objavljene e-naslove, in tržne raziskave pošiljajo brez vnaprejšnje privolitve, lahko zelo jasno uvrstimo med sporočila, ki so **posredno namenjena promociji**, še posebej vsakič, ko je tržna raziskava vezana na nek otipljiv produkt, osebo, storitev. Prav tako je opazen porast **politično promocijskih** elektronskih sporočil, ki se pošiljajo brez vnaprejšnje privolitve prejemnikov. Kot je razvidno iz zgornjih definicij, neposredno trženje zajema tudi promocije oseb, ki opravljajo določeno dejavnost. Promocija političnih osebnosti in strank tako zelo jasno sodi v definicijo neposrednega trženja.

Iz tega podrobnega pojasnila in analize ostale zakonodaje, ki velja za iste osebe in zavezance ter ista dejanja, in **bi torej morala biti zaradi pravne varnosti in učinkovitega izvajanja zakonodaje vsaj usklajena (če že zajeta v različnih zakonih)**, je razvidno, da neposredno trženje nikakor ni omejeno le na trženje v smislu komercialnega odnosa kupec – prodajalec, pač pa je to lahko raznovrstna, tudi posredna, promocija, ki ji izvajajo raznovrstne organizacije, tudi politične.

Zaradi navedenega in zaradi predlagane določbe, da se ob hkratni kršitvi ZEPT in ZEKom-1 uporablja slednji, **znova predlagamo in vztrajamo pri tem**, da se v okviru ZEKom-1 jasneje določi, kaj zajemajo **»nameni neposrednega trženja«**, oziroma da se teh namenov ne enači zgolj s komercialnimi nameni v odnosu kupec-prodajalec. Menimo, da bi morali določbe omenjenih Direktiv in ZEPT pri spremembah ZEKom upoštevati. V nasprotnem primeru bo situacija nejasna, prav tako pa bodo nejasne pristojnosti za nadzor v primeru neposrednih trženjskih sporočil, ki niso, z vašimi besedami, »komercialnega namena« pač pa bi spadala v področje drugih mogočih komercialnih sporočil, znotraj definicije v ZEPT.

Zato predlagamo, da se določba popravi bodisi na način, kot smo ga predlagali v prejšnjem mnenju, torej:

Uporaba avtomatičnih klicnih in komunikacijskih sistemov brez človekovega posega (klicni avtomati), faksimilnih naprav (faksov) ali elektronske pošte ***za namene neposrednega trženja, raziskovalne namene in namene politične promocije*** *je dovoljena samo za naročnike ali uporabnike, ki v to prej privolijo.*

Bodisi na način, da se **ZEKom glede definicije neposrednega trženja v obrazložitvi sklicuje na zgornje definicije neposrednega trženja iz Direktive 95/46/EC in Direktive 2000/31/EC (oz. ZEPT), iz katerih zelo jasno izhaja, da spada v neposredno trženje kakršna koli promocija.** Na ta način bo pošiljanje neželene elektronske pošte veliko bolj enotno in pregledno urejeno, jasnejše pa bodo tudi pristojnosti glede nadzora nad kršitvami pri pošiljanju fizičnim osebam:

(šesti odstavek)
Določilo določa predpis, ki se uporablja za nadzor nad neželeno elektronsko pošto; in glasi:
»Kadar se pošiljajo komercialna sporočila po elektronski pošti v nasprotju z določbami tega člena in gre hkrati tudi za nezaželeno elektronsko pošto skladno z zakonom, ki ureja varstvo potrošnikov, se uporabijo določbe tega zakona.«

Opozarjamo, da popolnoma enako določa tudi ZEPT v tretjem odstavku 6. člena, in sicer:
»Kadar se pošiljajo komercialna sporočila v nasprotju s prvim in drugim odstavkom tega člena ter gre hkrati tudi za neželeno elektronsko pošto v skladu z zakonom, ki ureja varstvo potrošnikov, se uporabijo določbe tega zakona.«

Torej še vedno ni jasno, kateri zakon se uporabi, če gre za nezaželena komercialna elektronska sporočila fizični osebi. Predlagamo, da dikcijo spremenite, tako da glasi:
»Kadar se pošiljajo komercialna sporočila fizični osebi po elektronski pošti v nasprotju z določbami tega člena in zakona, ki ureja elektronsko poslovanje na trgu in gre hkrati tudi za nezaželeno elektronsko pošto skladno z zakonom, ki ureja varstvo potrošnikov, se uporabijo določbe tega zakona.«

Predlagamo predvsem, da se v obrazložitvi jasno pove, da je za nadzor nad nezaželeno komercialno elektronsko pošto fizični osebi pristojen APEK (in ne TIRS). Nadzor nad pošiljanjem nezaželene komercialne elektronske pošte pravnim osebam pa opravlja (po ZEPT) TIRS.

K 159. členu
V zvezi s 159. členom bi radi opozorili na, po našem mnenju, neustrezno prevajanje termina »personal data breach« iz Direktive 136/2009 v »kršitev **zavarovanja** osebnih podatkov«. Slovenski prevod Direktive uporablja termin »kršitev **varnosti** osebnih podatkov«. Menimo, da sta oba prevoda neustrezna, in predlagamo, da se termin prevaja kot »kršitev **varstva** osebnih podatkov«.
Termin varstvo osebnih podatkov se uporablja širše in je bolj ustaljen, ko govorimo o pravici posameznika do **varstva osebnih podatkov**. Ta pravica je kršena, ko zaradi neustreznega zavarovanja pride do nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, kot je to opredeljeno v uvodnih definicijah. Pojem varstvo je v tem kontekstu širše narave kot pojem zavarovanje. V ZVOP-1 je zavarovanje opredeljeno le kot del pravice do varstva osebnih podatkov in enako razmerje bi moralo biti vključeno v ZEKom-1. Zavarovanje pomeni različne vrste ukrepov, s katerimi se zagotovi, da do podatkov ni mogoč nepooblaščen dostop in njihova integriteta, varstvo osebnih podatkov pa je termin, s katerim je poimenovana pravica posameznika, ki je lahko kršena zaradi neustreznega zavarovanja.

K 160. členu (peti odstavek)

Člen določa, da morajo operaterji skupaj s pristojnimi organi, ki izvajajo nadzor komunikacij, zagotoviti *tridesetletno neizbrisno registracijo* vsakega zakonitega prestrezanja komunikacij in morajo v okviru tega roka hraniti zbrane podatke ter jih varovati skladno z oznako stopnje tajnosti prepisa odredbe.

Člen sicer ne odstopa bistveno od veljavne ureditve v 107. členu ZEKom (šesti odstavek), razen dostavka, da operaterji *skupaj* s pristojnimi organi, ki izvajajo nadzor komunikacij. Če to pomeni, da bo podatke dejansko hranil pristojni organ (in ne operater), bi bilo to po mnenju Pooblaščenca sicer primerno, vendar ne glede roka hrambe (že sedaj je bil prekomeren in v neskladju s področnimi zakoni, ki urejajo delovanje pristojnih organov), ki določa, da se ti podatki hranijo neizbrisno (trideset let). Pooblaščenec opozarja, da so roki hrambe že določeni v področnih predpisih, ki urejajo delo pristojnih organov – organov, ki lahko odredijo nadzor komunikacij. Tako npr. Zakon o kazenskem postopku v 154. členu natančno določa roke hrambe podatkov, pridobljenih z izvedbo prikritih ukrepov (med katere sodi tudi zakonito prestrezanje komunikacij) in napotuje na uporabo pravil, ki veljajo za hrambo kazenskih spisov – Pravilnik o izločanju dokumentarnega gradiva. Posebej opozarjamo na dejstvo, da se po zakonu o kazenskem postopku v primerih, ko se tožilec odloči, da ne bo začel kazenskega pregona gradivo (pridobljeno s posebnimi ukrepi) pod nadzorom preiskovalnega sodnika uniči. Upoštevaje ZEKom pa bi hranili tudi gradivo (podatke o komunikacijah), na podlagi katerih kazenski postopek niti ni bil izpeljan.

Pooblaščenec tako opozarja, da določba o roku hrambe podatkov, pridobljenih ob nadzoru komunikacij ni primerna. Predlagamo, da se spremeni, tako da glasi:
»Operaterji morajo zagotoviti tridesetletno neizbrisno registracijo vsakega zakonitega prestrezanja komunikacij, ki vključuje podatke iz prvega oziroma četrtega odstavka tega člena in podatke o izvršitvi odredbe (kdo jo je izvršil, trajanje prestrezanja) ter jih varovati skladno z oznako stopnje tajnosti prepisa odredbe. S prestrezanjem pridobljene podatke o komunikacijah morajo operaterji izročiti organu, ki je prestrezanje odredil. Organ hrani podatke v skladu s predpisom, ki ureja njegovo delovanje.«

K 250. členu

Člen uvaja prehodno določbo za prilagoditev glede uporabe piškotkov. Pooblaščenec prehodno obdobje pozdravlja, menimo, da vsekakor potrebno, saj bo nova določba povzročila precejšnje spremembe na trgu ponudnikov storitev. Glede na izkušnje drugih držav članic, ki so določbo Direktive o piškotkih že implementirale v nacionalno zakonodajo (npr. Velika Britanija in Nizozemska) in glede na tehnično zahtevnost prilagajanja novi določbi predlagamo, da se prehodno obdobje podaljša na **5 mesecev od sprejetja zakona.**

Lepo vas pozdravljamo,

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