UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Alja Stanko

Prenos Direktive 95/46/ES in politika varovanja osebnih podatkov

Diplomsko delo

Ljubljana, 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Alja Stanko

Mentor: izr. prof. dr. Damjan Lajh

Prenos Direktive 95/46/ES in politika varovanja osebnih podatkov

Diplomsko delo

Ljubljana, 2011

Prenos Direktive 95/46/ES in politika varovanja osebnih podatkov

Posameznik je vsakodnevno lahko izpostavljen zlorabi osebnih podatkov, zato je bilo potrebno to področje zakonsko podrobneje urediti. S tem namenom je bila sprejeta Direktiva 95/46/ES v okviru Evropske unije, nato pa še Zakon o varstvu osebnih podatkov, ki je prenesel omenjeno direktivo v slovenski pravni red. Ker je varovanje osebnih podatkov vedno bolj pomembno je bil v skladu z Direktivo ustanovljen tudi neodvisen organ, ki zagotavlja spoštovanje pravil na področju varstva osebnih podatkov. Informacijski pooblaščenec izvaja inšpekcijski nadzor nad izvajanjem zakonskih določb o varstvu osebnih podatkov, ter s tem vpliva na samo implementacijo politike varovanja osebnih podatkov, v okviru svojega delovanja, pa poleg mednarodnega delovanja, nadzora zakonitosti obdelave osebnih podatkov, izdaje različnih mnenj in priporočil ter pisanja strokovnih člankov vsako leto izda tudi letno poročilo, ki predstavlja pregled nad implementacijo politike varovanja osebnih podatkov. Hitremu razvoju tehnologije pa pravni okvir le stežka, zato postajajo pomembni tudi preventivni mehanizmi, kot je na primer presojanje vplivov na zasebnost, ki jih prav tako izvaja Informacijski pooblaščenec.

Ključne besede: varstvo osebnih podatkov, informacijski pooblaščenec, Direktiva 95/46/ES, informacijska zasebnost.

Adaptation of Directive 95/46/EC and data protection policy

Individuals may be daily exposed to abuse of personal data therefore it was necessary to regulate this area. To this end, Directive 95/46/EC was adapted within the European Union, followed by the Law on the protection of personal data which transferred the Directive into Slovenian law. As protection of personal data is increasingly becoming more and more important an independent body, which ensures compliance with the Slovenian law on the protection of personal data, was established. Information Commissioner carries out inspections of the implementation of legal provisions on data protection and with that it influences implementation of data protection policy. Information Commissioner, within the framework of his competences, in addition to international cooperation, control of the processing of personal data, issuing opinions and recommendations and writing scientific articles, publishes annual reports presenting an overview of the implementation of data protection policy. Regulatory framework hardly follows the rapid development of technology therefore preventive measures, such as privacy impact assessment, are becoming very important.

Key words: data protection, information commissioner, Directive 95/46/ES, information privacy.

KAZALO

KAZALO SLIK

1 UVOD

> *Človekove pravice, med katere spada tudi pravica do zasebnosti, so najstarejše pravice, ki jih država ne more podeljevati ne pogojevati, ker pripadajo človeku že samo zaradi dejstva, da je človek. Te pravice pravna teorija označuje kot absolutne pravic, pogosto tudi kot univerzalne. To pomeni, da veljajo v vsakem primeru in zoper vsakogar, pri čemer pravice ne bi smele biti odvisne od sprotne zakonodajalčeve subjektivne volje. To jim daje naravo nevtralnosti. Čeprav je pravica do zasebnosti ena temeljnih človekovih pravic, ne deli v celoti tudi njihove usode. Nekatere osebnostne pravice so take, da jih predvsem moderne demokratične družbe priznavajo v celoti in brez priziva, saj so jasno opredeljene in pravno umeščene. Zasebnost pa je bistveno bolj izmuzljiva* (Cvetko 1999, 15–16).

Enotne opredelitve zasebnosti ni, to pa pomeni različno pravno umestitev in oteženo pravno varstvo. Wagner DeCewova na primer govori o treh vrstah zasebnosti, ki se med seboj mnogokrat prekrivajo: informacijski zasebnosti, zasebnosti dostopnosti ter zasebnosti izražanja. »Informacijska zasebnost obsega varovanje informacij o posamezniku, z njegovimi komunikacijami vred, ogrožena pa je z zbiranjem in objavo osebnih podatkov brez soglasja posameznika, prisluškovanjem in opazovanjem ali pa tudi samo s poskusi teh dejanj« (Wagner DeCew v Kovačič 2006, 45). Pri zasebnosti dostopnosti gre za možnost posameznika, da je sam; da nihče ni pozoren nanj in da nihče nima o posamezniku niti informacij niti fizičnega pristopa do njega (Kovačič 2006, 46). Zasebnost izražanja pa se nanaša na avtonomijo posameznika, da svobodno izbira stike, življenjski slog, načine delovanja in da posameznika ščiti pred pritiski okolice.

Podobno delitev pojma zasebnosti uvede tudi Čebulj (1992, 7), ki navaja tri sestavine zasebnosti, in sicer zasebnost v prostoru, zasebnost osebnosti in informacijsko zasebnost. Za razliko od Čebulja, pa Lampe, ki izhaja iz 8. člena Evropske konvencije o človekovih pravicah, pravico do zasebnosti deli na področje, ki pokriva zasebno in družinsko življenje, dom in dopisovanje (Lampe 2004, 49). V diplomskem delu bom obravnavala informacijsko zasebnost, ki je po navedbah Brezovška in Črnčeca (2007, 195) sinonim za varstvo osebnih podatkov in ena od sestavin zasebnosti.

K hitremu razvoju pravice do zasebnosti je v največji meri pripomogel razvoj tehnologije. Tehnološke spremembe namreč vsakodnevno prinašajo nove oblike in načine posegov v zasebnost, pravo pa je na te spremembe prisiljeno reagirati. Pravzaprav pravni sistem tem tehnološkim spremembam poskuša slediti (Sykes v Kovačič 2006, 46), zato gre pri razvoju

pravice do zasebnosti za nenehno prilagajanje načel varstva zasebnosti tehnološkim spremembam (Kovačič 2006, 46).

Pri varovanju osebnih podatkov, se ob hitrem razvoju informacijske tehnologije vsakodnevno srečujeta dva nasprotujoča si interesa, in sicer želja do neomejenega dostopa do informacij na eni strani, ter želja po varstvu informacij o določenem posamezniku na drugi. »Država zaradi izvajanja svojih funkcij potrebuje nekatere osebne podatke o svojih državljanih, pri tem pa trčita interes države za zbiranje, obdelovanje in shranjevanje osebnih podatkov ter interes posameznika po ohranjanju osebne integritete« (Brezovšek in Črnčec 2007, 196). Ker informacijska tehnologija danes omogoča vse bolj subtilne posege v zasebnost posameznika, obenem pa je možno v kratkem času obdelati neznanske količine podatkov, je bila ureditev tega področja nujno potrebna. Udejanjila se je v posebni javni politiki, ki je določila enotna načela, pravila in obveznosti tako na nadnacionalni kot nacionalni ravni.

Koncept varstva osebnih podatkov v Sloveniji temelji predvsem na določbi 38. člena Ustave, po kateri je varstvo osebnih podatkov ena izmed ustavno zagotovljenih človekovih pravic. Določba 38. člena Ustave torej zagotavlja varstvo osebnih podatkov, prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, vsakomur zagotavlja pravico do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, ter pravico do sodnega varstva ob njihovi zlorabi. Od leta 1990, ko je Slovenija dobila prvi zakon, ki je urejal varstvo osebnih podatkov, je bilo to področje še dvakrat reformirano (Likar 2009, 1). Vsaka od sprememb je prinesla večjo zahtevnost in natančnost pri ravnanju z osebnimi podatki in nekatere nove institute.

V diplomskem delu se bom raziskovanja področja varstva osebnih podatkov lotila v skladu s strukturo diplomskega dela. Uvodnemu delu bo sledil metodološki načrt dela, kjer bom natančneje opredelila cilj diplomske naloge in metode in tehnike, ki jih bom uporabila pri raziskovanju. Sledila bo analiza normativne ureditve področja varstva osebnih podatkov, ter predstavitev pristojnosti in dela Informacijskega pooblaščenca. Po obširni predstavitvi normativne ureditve, bom analizirala še letna poročila Informacijskega pooblaščenca in ugotovitve povzela v zaključku.

2 METODOLOŠKI OKVIR

2.1 Teoretična izhodišča

William Dunn (1994, 85) pravi, da je javna politika kompleksen vzorec bolj ali manj povezanih odločitev, vključno z odločitvami ne delovati, ki jih sprejmejo vladna telesa in uradniki. Javna politika oziroma posamezni javni program znotraj javne politike predstavlja neke vrste politični dogovor o dejavnostih, pa tudi nedejavnostih, ki jih država oblikuje z namenom reševanja ali blažitve problemov, ki se pojavljajo na političnem dnevnem redu (Fischer 2006, 2). Javne politike so politične odločitve oziroma uradna pravila obnašanja, ki so zavezujoča na teritoriju, ki ga upravlja in nadzoruje pristojna državna avtoriteta. Odločanje o javnih politikah je monopol političnih odločevalcev, ki odločajo tudi o uporabi instrumentov in mehanizmov za izvajanje javnih politik (Fink Hafner 2007, 15). Vsaka javna politika ima tudi neke vrste življenjski cikel, sestavljen iz opredelitve problema, izbora alternativne rešitve, njene uzakonitve, izvajanja ter končno vrednotenja načinov in učinkov omenjenega izvajanja (Kustec Lipicer 2007, 31).

Implementacija je izvajanje osnovnih javnopolitičnih odločitev, ki so navadno sprejete v obliki nekih pravil, lahko tudi odločitev sodišča. V idealnih razmerah te odločitve identificirajo nastale probleme, opredelijo temeljne cilje in na različne načine strukturirajo proces implementacije (Lajh 2007, 158). Politika varovanja osebnih podatkov se je v okviru Evropske unije »udejanjila« s sprejetjem Direktive 95/46/ES, v Sloveniji pa je bil na področju varstva zasebnosti sprejet krovni Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1)[1], ki se izvaja zadnjih šest let, tako da se bom v diplomski nalogi osredotočila na vrednotenje implementacije navedenega zakona.

Ker gre za vrednotenje obstoječe javne politike, ki se še izvaja gre za programsko evalvacijo, za katero je značilno, da raziskuje uspešnost oziroma učinkovitost programov in javnih politik, s čimer omogoča tudi njihovo izboljšanje. Pomembno je namreč, da se javne politike, katerih izvajanje je še vredno truda loči od neučinkovitih ter da se uvedejo nove javne politike ali samo popravijo obstoječe (Rossi in drugi 2003, 16). Vrednotenje programov je torej potrebno predvsem zaradi omogočanja sprotnih popravkov zastavljenega programa,

[1] Zaradi poenostavitve uporabljam kratico ZVOP-1 za navajanje uradnega prečiščenega besedila Zakona o varstvu osebnih podatkov.

omogočanja nadaljevanja, razširitve, institucionalizacije programa ali pa njegovo oklestenje, prenehanje oziroma ukinitev, omogočanje preverjanja novih programskih idej in izbiro najboljše izmed številnih možnosti (Kustec Lipicer 2007, 30).

Po besedah Carol H. Weiss (1998, 4) je vrednotenje sistematično ocenjevanje operacij ali rezultatov nekega programa ali politike. Rezultate nato primerjamo z naborom eksplicitnih in implicitnih standardov postavljenih z namenom pomagati pri izboljšavi programa oziroma politike. Upoštevajoč slednjo definicijo je potrebno določiti tudi standard, ki bo v mojem primeru uspešnost ukrepov javne politike varstva osebnih podatkov. Ker je za vsako evalvacijsko študijo pa je izrednega pomena izbor kriterijev (Vedung 2005, 10), je potrebno določiti tudi te. Sama bom kot kriterij uporabila število prijavljenih sumov kršitev informacijske zasebnosti, delež zaprosil za mnenja ter število prekrškov med leti 2006 in 2010.

2.2 Cilj diplomskega dela

Cilj diplomske naloge je ugotoviti ali obstoječi ZVOP-1 zagotavlja ustrezno varnost posameznikove zasebnosti. V skladu z napisanim se bom osredotočila na uspešnost pri kateri, za razliko od učinkovitosti, niso pomembni stroški, ampak nas zanima stopnja do katere rezultati dosegajo cilje (Vedung 2005, 258). Ker gre pri programski evalvaciji predvsem za zbiranje informacij in interpretacijo teh z namenom odgovoriti na vprašanja povezana z izbranim programom in njegovo uspešnostjo, je pomemben korak pri evalvaciji tudi oblikovanje vprašanj na katera želimo najti odgovor (Rossi in drugi 2003, 52–53). S pomočjo evalvacije želim ugotoviti:

- kako veliko je bilo število prijav zaradi suma kršitev ZVOP-1 in koliko le-teh je bilo ugotovljenih med leti 2006 in 2010 ter koliko zaprosil za mnenja je bilo vloženih;

- ali v primeru pravne praznine znotraj zakona obstajajo določeni podzakonski akti, ki natančneje določajo, kaj vse se definira kot kršitev in poseg v posameznikovo integriteto ter dodatno definirajo pristojnosti Informacijskega pooblaščenca;

- ali bi bilo potrebno področje varstva osebnih podatkov zakonsko natančneje urediti, tako na nacionalni kot tudi na evropski ravni.

Cilj bom poskušala doseči s pomočjo naslednje hipoteze: *Zaradi vedno boljšega poznavanja področja varstva osebnih podatkov državljani vlagajo vedno več zaprosil za mnenja in sprožajo vedno več postopkov pred Informacijskim pooblaščencem*.

2.3 Metode in tehnike

Po navedbah Maychrzakove je za raziskovanje zastavljenega problema potrebno združiti različne metodološke pristope, ki širijo verodostojnost zbranih podatkov (Maychrzak 1984, 66). V ta namen bom v diplomski nalogi najprej uporabila analizo primarnih virov, v okviru le-te se bom osredotočila predvsem na Zakon o varstvu podatkov, kot na osrednji dokument slovenske zakonodajne ureditve omenjenega področja, in Direktivo 95/46/ES, ki zavezuje države članice Evropske unije, da zagotovijo določeno varnost pri ravnanju z osebnimi podatki. Ker se posledic političnih odločitev ne da natančno predvideti je pri implementaciji določene javne politike potrebno tudi spremljanje ali *monitoring* (Grdešić 2006, 133); saj z njim pridemo do informacij o posledicah in učinkih sprejete javne politike (Dunn 1994, 19).

Kot navaja Grdešić (2006, 35) je pri odkrivanju in definiranju problema potrebno preučiti do takrat znane podatke. Zbrani material je nato potrebno sistematizirati in pripraviti za nadaljnjo klasifikacijo oziroma analizo, zatorej bom pri preučevanju uporabila tudi analizo sekundarnih virov. To je metoda, ki uporablja že obstoječe informacije, zanjo pa je značilno, da ima raziskovalec z njo zelo nizke stroške (Maychrzak 1984, 60). V diplomskem delu bom tako analizirala različne strokovne članke in monografije, ki se nanašajo na pravico do zasebnosti oziroma pravico do varstva osebnih podatkov.

Na koncu bom uporabila še družboslovni intervju, ki je kvalitativna metoda in nezamenljiv način pridobivanja tistih podatkov, ki jih ni možno pridobiti iz literature, dokumentov, internetnih strani (Grdešić 2006, 64). Intervju bom opravila s predstavnikom Ministrstva za notranje zadeve, kjer imajo omogočen dostop do številnih »občutljivih« podatkov ter različnih evidenc. Prav tako bom opravila intervju s predstavnikom zdravstvene ustanove, kjer obdelujejo številne osebne podatke svojih pacientov, na koncu pa še s predstavnikom Informacijskega pooblaščenca.

3 NORMATIVNA UREDITEV

Varstvo osebnih podatkov oziroma informacijska zasebnost zajema pravice posameznika pred nezakonitimi in neupravičenimi posegi v njegovo zasebnost (Kaučič in Grad 2003, 122). Za normativno urejanje varstva osebnih podatkov v Sloveniji je pomemben drugi odstavek 38. člena Ustave, v katerem je določeno, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Po navedbah Letnega poročila Informacijskega pooblaščenca (2010, 29) gre za t. i. obdelovalni model z določenimi pravili za urejanje dopustne obdelave osebnih podatkov na zakonski ravni. Po tem modelu je na področju obdelave osebnih podatkov prepovedano vse, razen tistega, kar je z zakonom (na področju zasebnega sektorja tudi z osebno privolitvijo posameznika) izrecno dovoljeno. Poseg v z ustavo varovano človekovo pravico do varstva osebnih podatkov, je torej dopusten, le če je v zakonu opredeljeno, kateri osebni podatki se smejo obdelovati, obenem pa mora biti jasno določen tudi namen obdelave osebnih podatkov, zagotovljeno mora biti ustrezno varstvo in zavarovanje osebnih podatkov. Namen obdelave osebnih podatkov mora biti ustavno dopusten, obdelovati pa se smejo le tisti osebni podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega in ustavno dopustnega namena.

Izbrani javnopolitični problem varstva osebnih podatkov tako posredno in neposredno urejajo številni pravni akti na nacionalni in nadnacionalni ravni. Temeljne pravne podlage slovenske zakonske ureditve varstva osebnih podatkov so Ustava Republike Slovenije, Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija 108), ki je bila leta 1981 sprejeta v okviru Sveta Evrope in jo je Slovenija ratificirala leta 1994 ter Direktiva 95/46/ES Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Bien Karlovšek in drugi 2006, 4/1).

3.2 Direktiva o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov 95/46/ES

> *Ustava Republike Slovenije v 3.a členu določa, da lahko Slovenija z mednarodno pogodbo, ki jo ratificira državni zbor z dvotretjinsko večino glasov vseh poslancev, prenese izvrševanje dela suverenih pravic na mednarodne organizacije, ki temeljijo na spoštovanju človekovih pravic in temeljnih svoboščin, demokracije in načel pravne države. Pravni akti in odločitve, sprejeti v okviru mednarodnih organizacij, na katere Slovenija prenese izvrševanje dela*

suverenih pravic, se v Sloveniji uporabljajo v skladu s pravno ureditvijo teh organizacij (Kotnik Šumah 2006, 9).

Za področje splošne ureditve varovanja zasebnosti in osebnih podatkov je najpomembnejše določilo 8. člena Evropske konvencije o človekovih pravicah in temeljnih svoboščinah, ki zahteva od državne oblasti varovanje pravice do zasebnosti tako pred neposrednimi vplivi njenih organov kot zahteva, da s svojimi zakonodajnimi instrumenti zagotovi učinkovit sistem varstva tudi med zasebnim sektorjem in posamezniki. Zatem je Svet Evrope sprejel še specialno Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je posredno vplivala tudi na kasnejši sprejem Direktive 95/46/ES.

Pravni red Evropske unije temelji na ustanovitvenih pogodbah, dopolnjujejo pa ga pravni viri, ki jih sprejemajo institucije Evropske unije. »To so uredbe, ki so splošno veljavne ter se v državah članicah uporabljajo neposredno, direktive, ki države članice zavezujejo k opredeljenemu cilju, ne določajo pa zakonodajnih sredstev za njihovo uresničitev, ter odločbe, ki so v celoti zavezujoče za vse, na katere so naslovljene« (Kotnik Šumah 2006, 9). Da bi odstranila morebitne ovire pretoka osebnih podatkov in zagotovila visoko raven zaščite v Uniji, sta Evropski parlament in Svet z zaščito osebnih podatkov povezano zakonodajo harmonizirala v že prej omenjeni Direktivi o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov. »Direktiva zavezuje vsako državo članico, na katero je naslovljena, za rezultate, ki jih je treba doseči, organom oblasti pa prepušča presojo o uporabi oblik in metod« (Bohinc 2007, 44).

Leta 1995 je, kot je bilo že omenjeno, Evropska unija sprejela Direktivo 95/46/ES. Kot navaja Kovačič (2006, 78) je bil prvi osnutek pripravljen že leta 1990, vendar je predvideval drugačno obravnavo osebnih podatkov v javnem in zasebnem sektorju. Leta 1992 je Evropski parlament sprejel dopolnilo, s katerim je osebne podatke v javnem in zasebnem sektorju izenačil. Leta 1997 je bila v Evropski uniji sprejeta tudi Direktiva o zasebnosti telekomunikacij 97/66/ES, leta 2002 pa Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/ES. Obe direktivi sta nekoliko bolj konkretizirali varstvo zasebnosti na področju telekomunikacij in elektronskih komunikacij (Kovačič 2006, 82) in s tem še natančneje definirali pojem nedovoljenih posegov v zasebnost posameznika.

Direktiva 95/46/ES (v nadaljevanju Direktiva), ki je osrednji evropski pravni akt na področju varovanja zasebnosti, ima dva integralna dela. Prvi je uvodni oziroma pojasnjevalni in ima 72 točk. Sestavljen je iz treh vsebinskih sklopov, in sicer iz preambule, opredelitve temeljnih

ciljev in interpretacijskih napotkov. Drugi del pa je normativni in ima 34 členov, ki so razdeljeni v sedem poglavij.

V prvem poglavju z naslovom Splošne določbe so opredeljeni cilji Direktive, glavne definicije, področje učinkovanja ter uporaba nacionalnega prava. Direktiva se nanaša tako na avtomatsko obdelavo, kot tudi na klasično obdelovanje osebnih podatkov. Najobsežnejše je drugo poglavje, ki se nanaša na opredelitev pojmov zakonitosti obdelovanja osebnih podatkov. Navedeno poglavje je sistematično razdeljeno na devet oddelkov, ki predstavijo temeljna načela varstva osebnih podatkov v Evropski uniji.

Če povzamemo po direktivi je najprej v sedmem členu navedeno načelo zakonitosti, ki določa, da je obdelava osebnih podatkov zakonita samo, če posameznik vanjo nedvoumno privoli, v drugih primerih pa je to mogoče le če ima upravljavec zbirke podatkov za to pooblastilo v zakonu, če je obdelava nujna za izpolnitev njegovih nalog ali če je nujna zaradi varstva javne koristi, če je obdelava nujna zaradi varstva posameznika, na katerega se podatki nanašajo ali če je obdelava nujna zaradi izvrševanja pravnih poslov, v katerih je udeležen posameznik. Sledi načelo predhodne določitve namena, ki zahteva, da se podatki obdelujejo praviloma samo za vnaprej eksplicitno določene namene.

Načelo relevantnosti preprečuje prekomernost pri zbiranju osebnih podatkov, saj zahteva sorazmerje med količino zbranih podatkov in namenom njihove obdelave - zbirajo naj se le nujno potrebni podatki. Načelo kvalitete podatkov zahteva točnost zbranih podatkov in njihovo ažurnost. Naslednje načelo je načelo časovne omejitve, ki omejuje shranjevanje osebnih podatkov v obliki, ki omogoča identifikacijo posameznika na čas, ki je nujno potreben za dosego namena, za katerega so bili podatki zbrani. Načelo zavarovanja, ki je povzeto v 16. in 17. členu Direktive, govori o tehničnih in drugih ukrepih, s katerimi naj bi se nepooblaščenim uporabnikom preprečil dostop do podatkov. Načelo svobodnega pretoka prek državnih meja pa izhaja iz zahtev skupnega evropskega trga po svobodnem pretoku blaga, storitev, oseb in kapitala. V okviru tega so prikazana tudi izhodišča za skupni evropski informacijski trg.

»Načelo notifikacije od držav članic zahteva, da v nacionalni zakonodaji upravljalcu zbirke osebnih podatkov naložijo obveznost, da morajo zato določeni državni organ obvestiti o tem, da bodo pričeli z obdelavo določene vrste podatkov za določene namene. Načelo seznanjenosti posameznika pa zavezuje države članice, da predpišejo obveznost upravljalcu zbirke podatkov, da posameznika seznani z zbiranjem in obdelavo podatkov« (Čebulj 1996,

31). Drugo poglavje med drugim določa tudi izjeme in omejitve, pravico posameznika do ugovora in obveznost uradnega obveščanja nadzornega organa.

Tretje poglavje se nanaša na določitev pravnega sredstva, odgovornosti in sankcij v nacionalnih zakonodajah. V 22. členu je določeno, da morajo države članice vsakomur zagotoviti pravico do sodnega varstva v primeru kršitev predpisov o varstvu osebnih podatkov, hkrati pa morajo države članice posamezniku zagotoviti tudi pravico do odškodnine v primeru nastanka škode zaradi kršitev informacijske zasebnosti (23. člen). Direktiva s tem zavezuje države članice, da v svoji zakonodaji določijo ustrezne pravne sankcije za primere kršitev informacijske zasebnosti posameznika.

Četrto poglavje Direktive se nanaša na prenos osebnih podatkov v tretje države. Direktiva v svojem 25. členu določa, da bodo države članice v svoji zakonodaji predpisale, da je iznos osebnih podatkov možen samo v primeru, če je v posamezni državi zagotovljen primeren nivo zaščite osebnih podatkov. Določeno je tudi, da se posamezna država članica in Komisija Evropske unije medsebojno obveščata o zadevah in primerih, ko ena ali druga stran meni, da določena tretja država ne zagotavlja ustreznega nivoja varstva podatkov. Če bi komisija v posebnem postopku ugotovila, da to drži, bi morale države članice preprečiti vsakršen iznos podatkov v to državo.

Peto poglavje se nanaša na spodbujanje priprav kodeksov ravnanja pri obdelovanju osebnih podatkov, katerih namen je prispevati k pravilnemu izvajanju nacionalnih predpisov, ki so jih sprejele države članice v skladu s to Direktivo, ob upoštevanju značilnosti različnih področij (Evropski parlament in Svet, 27. čl.). Šesto poglavje določa obveznost ustanovitve dveh organov za varstvo informacijske zasebnosti posameznika, in sicer nadzornega organa na nacionalnem nivoju ter delovnega telesa za varstvo z vidika obdelovanja osebnih podatkov na nivoju Evropske unije.

V sedmem poglavju Direktiva predvideva ustanovitev posebnega odbora, čigar skrb je pomoč Komisiji Evropske unije pri sprejemanju operativnih ukrepov za izvajanje vsebine te Direktive. V končnih določbah je določeno še, da morajo države članice sprejeti vse potrebne ukrepe za uskladitev notranje zakonodaje s to Direktivo v treh letih od njenega sprejema. Države morajo Komisiji Evropske unije posredovati tekste nacionalnih predpisov, ki jih sprejemajo s ciljem uskladitve s to Direktivo. Komisija je prav tako zavezana, da mora v določenih intervalih poročati Svetu Evropske unije in Evropskemu parlamentu o problemih implementacije Direktive ter ob teh poročilih pripravljati tudi ustrezne dodatne predloge in

morebitne amandmaje k Direktivi. Z vidika spremljanja razvoja informacijske tehnologije je Komisija Evropske unije zadolžena tudi za proučevanje združljivosti Direktive z vidika obdelovanja posebnih osebnih podatkov t. i. zvokov in podob, ki se nanašajo na fizično osebo, kar je določeno v 33. členu. »Ta direktiva ima kar nekaj pomembnih določil, med drugim se ne nanaša samo na živeče posameznike, dovolj široko definira obdelavo osebnih podatkov, predvsem pa v 28. členu zahteva ustanovitev neodvisnega nadzornega organa, ki skrbi za spoštovanje zakonodaje za zaščito zasebnosti« (Kovačič 2006, 78).

3.1 Zakon o varstvu osebnih podatkov

Prvi zakon s področja varstva osebnih podatkov v Republiki Sloveniji je bil Zakon o varstvu osebnih podatkov, ki je začel veljati marca 1990. Kot navaja Čebulj (1996, 43) je bil omenjeni zakon razdeljen na dvanajst poglavij, njegov temeljni cilj pa je bil urediti varstvo osebnih podatkov in v tem okviru preprečiti nezakonit in čezmerni poseg v integriteto človekove osebnosti, ki je lahko posledica zbiranja, obdelave in shranjevanja osebnih podatkov ter njihove uporabe.

Zaradi približevanja Evropski uniji in zahtev Direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem gibanju podatkov je Državni zbor Republike Slovenije julija 1999 sprejel nov Zakon o varstvu osebnih podatkov, ki je začel veljati avgusta 1999. Novi zakon naj bi bil že usklajen z Direktivo, vendar pa se je izkazalo, da je pomanjkljiv, zato je bil leta 2001 sprejet Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov, ki je začel veljati julija 2001 (Likar 2009, 15). Namen novele je bil predvsem v uskladitvi zakona z Direktivo v določbah, ki se nanašajo na neodvisni nadzorni organ za varstvo osebnih podatkov.

Sedaj veljavni Zakon o varstvu osebnih podatkov je bil sprejet julija 2004 in je začel veljati 1. januarja 2005. »Potreben je bil predvsem zaradi določb evropskega pravnega reda, spet Direktive, saj je sodna praksa Sodišča Evropskih skupnosti leta 2003 ugotovila, da so vsebine določb tako podrobne, da jih morajo države članice sprejeti z natanko tako vsebino« (Letno poročilo Informacijskega pooblaščenca 2010, 30). Julija 2007 je bila sprejeta novela ZVOP-1, ki je uvedla dve pomembni novosti, in sicer z vidika administrativnih razbremenitev upravljavcev osebnih podatkov ter predpisovanja določenih olajšav z vidika oblik dostopa

posameznikov do njihovih osebnih podatkov v register in je prinesla določene pozitivne rešitve, predvsem olajšave za posameznike, na katere se osebni podatki nanašajo.

3.1.1 Splošne določbe (1. - 7. člen)

V prvem členu sta opredeljena vsebina in namen tega zakona. Določeno je, da se s tem zakonom določajo pravice posameznika, obveznosti obdelovalca osebnih podatkov, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo pri obdelavi podatkov.

> *ZVOP-1 izhaja iz načel v 38. členu Ustave RS, in seveda iz načel v Konvenciji in Direktivi. Zakonodajalec se je namreč odločil za sprejetje novega zakona, ki ureja varstvo osebnih podatkov, prav z namenom, da bi v celoti implementiral določbe omenjenih dokumentov v slovenski pravni red. To pomeni, da zakon v celoti temelji na načelih za varstvo podatkov, vsebovanih v direktivi in s tem tudi v Konvenciji. V okviru splošnih določb ZVOP-1 še posebej navaja tri načela: načelo zakonitosti in poštenosti, načelo sorazmernosti in načelo prepovedi diskriminacije* (Čebulj in Žurej 2005, 26).

Kot pravi Čebulj (2005, 27) je načelo zakonitosti in poštenosti primarno in najpomembnejše načelo, po katerem se morajo osebni podatki obdelovati zakonito in pošteno. Načelo sorazmernosti določa, da morajo biti osebni podatki, ki se obdelujejo ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Načelo prepovedi diskriminacije pa zagotavlja varstvo osebnih podatkov vsakemu posamezniku ne glede na raso, barvo kože, veroizpoved, etično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, premoženjsko stanje, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča ali katerokoli drugo osebno okoliščino.

V petem členu je določena ozemeljska veljavnost ZVOP-1. V dikcijo tega člena je implementiran 4. člen Direktive 95/46/ES, ki določa pogoje za uporabo nacionalne zakonodaje. Nadalje je razložen pomen izrazov kaj pomeni osebni podatek, kaj pomeni obdelava osebnih podatkov, kaj je avtomatizirana obdelava, kaj je zbirka osebnih podatkov, kdo je upravljalec osebnih podatkov, kaj je katalog zbirke osebnih podatkov ter kaj je register zbirk osebnih podatkov. Poznavanje teh izrazov je seveda bistveno za razumevanje določb tega zakona in ostalih aktov s področja politike varstva osebnih podatkov.

V sedmem členu ZVOP-1 so določene izjeme glede uporabe vseh ali dela tega zakona v določenih življenjskih situacijah, kjer bi bilo določbe tega zakona nesmiselno uporabljati. ZVOP-1 določa tri sklope izjem:

- prvi sklop se nanaša na obdelavo osebnih podatkov, ki jih posamezniki obdelujejo izključno v okviru svojega zasebnega življenja, v primeru izjem iz tega odstavka pa je izključena uporaba celotnega zakona;
- drugi sklop izjem se nanaša na osebne podatke, jih v svojih členih obdelujejo politične stranke, sindikati in verske skupnosti;
- tretja izjema pa se nanaša na osebne podatke, ki jih za namene obveščanja javnosti obdelujejo mediji.

3.1.2 Obdelava osebnih podatkov (8. - 28. člen)

Drugi del zakona je razdeljen na štiri poglavja. Začne se s splošno določbo glede določanja dopustne pravne podlage za obdelavo osebnih podatkov. Osebne podatke in njihovo obdelavo določa zakon ali pa mora biti podana izrecna privolitev posameznika. Nadalje je natančno razdelana pravna podlaga za obdelavo osebnih podatkov v javnem in zasebnem sektorju ter določene izjeme, kar je v skladu z določbami Direktive 95/46/ES. Zakon v nadaljevanju določa še, da mora biti posameznik, na katerega se nanašajo osebni podatki, predhodno pisno ali na drug način seznanjen z namenom njihove obdelave.

Upravljavec osebnih podatkov lahko posamezna opravila v zvezi z obdelavo podatkov s pogodbo zaupa pogodbenemu obdelovalcu. Pri tem je pomembno, da lahko obdelovalec osebnih podatkov podpiše pogodbo le s pravno osebo ali zasebnikom, ki izpolnjuje pogoje 24. člena ZVOP-1, ki so sledeči: pogodbeni obdelovalec mora biti registriran za opravljanje takšne dejavnosti; zagotavljati mora ustrezne organizacijske, tehnične in logično-tehnične postopke; medsebojne pravice in obveznosti morajo biti sklenjene v pogodbi, ki mora biti pisna.

»V tem delu je podana tudi podlaga za obdelavo osebnih podatkov v tistih primerih in življenjskih situacijah, ko je obdelava podatkov nujna za varovanje posameznikovega življenja ali telesa. V teh primerih se osebni podatki lahko zbirajo ne glede na to, da za obdelavo osebnih podatkov druga zakonita pravna podlaga ne obstaja« (Likar 2009, 18).

Občutljivi osebni podatki so najsubtilnejša kategorija osebnih podatkov, definirani so v šestem členu ZVOP-1, v tem delu zakona pa ja taksativno določenih osem pravnih podlag, ki dopuščajo njihovo obdelavo. Podlaga za določbo 13. člena ZVOP-1 je določba 8. člena Direktive, ki določa obdelavo občutljivih osebnih podatkov. Tam je zapisano, da države članice prepovedujejo obdelavo osebnih podatkov, ki kažejo na rasni etični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu in obdelavo osebnih podatkov v zvezi z zdravjem ali spolnim življenjem. Glede na to, da pomeni razkritje naštetih podatkov hud poseg v zasebnost posameznika, na katerega se podatki nanašajo, je treba zavarovanju obdelave občutljivih podatkov posvetiti še posebno pozornost.

ZVOP-1 ureja tudi avtomatizirano obdelavo podatkov, pri tem pa izrazito ščiti posameznika, ki je v obdobju modernih informacijskih tehnologij postal vse prevečkrat objekt obdelave. Osebni podatki se zaradi omejitve zlorab, lahko zbirajo le za določene in zakonite namene, zakon pa določa še, da se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Tu je vsebovano eno od temeljnih načel varstva osebnih podatkov t.i. načelo namenskosti.

V tem delu je urejeno tudi vodenje evidenc. Upravljalcu se nalaga, da za vsako zbirko osebnih podatkov, ki jo vodi in vzdržuje, vzpostavi katalog zbirke osebnih podatkov, pri tem pa ni relevantno, ali se zbirka osebnih podatkov vodi na podlagi zakona, na podlagi osebne privolitve posameznika, na podlagi pogodbenega razmerja ali pa na kakšni drugi pravni podlagi iz 9. in 10. člena ZVOP-1. Natančno je navedeno tudi, kaj katalog zbirke osebnih podatkov vsebuje ter da je upravljalec zavezan k skrbi za točnost in ažurnost podatkov. Upravljalec pristojnemu Državnemu nadzornemu organu za varstvo osebnih podatkov ni dolžan posredovati vseh podatkov iz katalogov zbirk osebnih podatkov, pač pa le tiste, ki mu jih določa 27. člen ZVOP-1. Register zbirk osebnih podatkov je v 13. točki prvega odstavka 6. člena ZVOP-1 definiran kot register, v katerem so podatki iz katalogov zbirk osebnih podatkov. Vsebuje torej tiste podatke, ki so jih nadzornemu organu iz svojih zbirk posredovali posamezni upravljalci. Na koncu je določeno tudi kdo register vodi in kje ga objavi.

3.1.3 Pravice posameznika (29. - 36. člen)

Tretji del se začne z določbo, da mora Državni nadzorni organ vsakomur dovoliti vpogled v register zbirk osebnih podatkov ter prepis podatkov. V skladu z Zakonom o informacijskem

pooblaščencu je to od 31. decembra 2005 obveznost Informacijskega pooblaščenca. Na podlagi tretjega odstavka 38. člena Ustave je zagotovljena pravica posameznika do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, kot tudi pravica do sodnega varstva ob zlorabi osebnih podatkov posameznika (ZVOP-1, 30. čl.). V 31. členu sledi navedba postopka za uveljavljanje prej omenjenih pravic.

»Pravice do dopolnitve, popravka, blokiranja, izbrisa in ugovora, so izraz pravice do informacijske samoodločbe, katere namen je zagotoviti transparentnost obdelave osebnih podatkov, s tem pa dobroverno in pošteno obdelavo osebnih podatkov. S tem se uresničuje temeljno načelo zakonitosti in poštenosti in 2. člena tega zakona« (Likar 2009, 19).

Posameznik, ki ugotovi, da so mu kršene pravice, določene s tem zakonom, lahko zahteva sodno varstvo ves čas, ko kršitev traja. Ta pravica izhaja iz 23. člena Ustave, po kateri ima vsakdo pravico, da o njegovih pravicah in dolžnostih ter obtožbah proti njemu brez nepotrebnega odlašanja odloča neodvisno, nepristransko in z zakonom ustanovljeno sodišče.

3.1.4 Institucionalno varstvo osebnih pravic (37. - 61. člen)

Inšpekcijski nadzor nad varstvom osebnih podatkov opravlja Državni nadzorni organ za varstvo osebnih podatkov. V zvezi z določbami o nadzornem organu je potrebno izpostaviti, da je decembra 2005 začel veljati Zakon o informacijskem pooblaščencu (v nadaljevanju ZInfP), ki je razveljavil določbe 1. poglavja četrtega dela ZVOP-1 ter združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel prej status neodvisnega organa in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje.

V nadaljevanju je določeno, da varuh človekovih pravic opravlja svoje naloge na področju varstva osebnih podatkov zgolj v razmerju do enega dela javnega sektorja. Varuh torej izvršuje svoje pristojnosti samo v razmerju do državnih organov, organov lokalnih skupnosti in nosilcev javnih pooblastil, ne pa tudi v razmerju do subjektov zasebnega sektorja (Čebulj in Žurej 2005, 40). Varuh v letnem poročilu državnemu zboru poroča o ugotovitvah, predlogih in priporočilih ter o stanju na področju varstva osebnih podatkov. Delovno telo državnega zbora, Odbor za notranjo politiko, javno upravo in pravosodje, spremlja razmere na področju varstva osebnih podatkov in se seznani z letnim poročilom in delom Informacijskega pooblaščenca, ki je glavni javnopolitični akter pri izvajanju politike varstva osebnih podatkov.

3.1.5 Iznos osebnih podatkov (72. - 90. člen)

Zakon loči med iznosom osebnih podatkov v države članice Evropske unije (EU) in Evropskega gospodarskega prostora (EGS) ter v države, ki to niso in jih zakon označuje kot tretje države. Za prvo skupino velja prost pretok podatkov. To pomeni, da se v primerih, ko se osebni podatki posredujejo upravljalcu, pogodbenemu upravljalcu ali uporabniku osebnih podatkov, ki je ustanovljen, ima sedež ali je registriran v državi članici EU ali EGS, določbe zakona o iznosu podatkov ne uporabljajo.

Iznos podatkov v tretjo državo pa je dopusten samo, če državni nadzorni organ izda odločbo, s katero ugotovi, da država, v katero se iznašajo podatki, zagotavlja ustrezno raven varstva osebnih podatkov. Opisan je postopek za ugotavljanje te ravni, državni nadzorni organ pa vodi seznam držav, ki jo zagotavljajo.

3.1.6 Področne ureditve (72. - 90. člen)

Zakon, v nasprotju s prejšnjim, vsebuje poseben del, ki ureja področne ureditve. V okviru tega vsebuje sedem poglavij, in sicer neposredno trženje, video nadzor, biometrijo, evidenco vstopov in izstopov iz prostorov, javne knjige, povezovanje zbirk osebnih podatkov ter strokovni nadzor. V sedanji potrošniško naravnani družbi, je za proučevanje zasebnosti in varstva osebnih podatkov posebej pomembna marketinška strategija, ki se imenuje neposredno trženje. Ta strategija zasebnost potencialno ogroža, zato je urejena tako v ZVOP-1 kot tudi v dodatnem zakonu in sicer Zakonu o elektronskih komunikacijah (Bien Karlovšek in drugi 2006, 4/13).

Z obdelavo biometričnih značilnosti se ugotavljajo ali primerjajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija oziroma preveri njegova identiteta, zato je tudi to področje izjemno občutljivo in posebej urejeno. Zbirke osebnih podatkov iz uradnih evidenc in javnih knjig je dovoljeno povezovati, če tako določa zakon. Upravljavci ali upravljavec osebnih podatkov, ki povezuje dve ali več zbirk osebnih podatkov, ki se vodijo za različne namene so dolžni o tem predhodno obvestiti Informacijskega pooblaščenca. Zakon, glede strokovnega nadzora določa, da se njegove določbe o strokovnem nadzoru uporabljajo subsidiarno v razmerju do področnih zakonov. »Bistvo strokovnega nadzora je v tem, da se v dejavnostih, ki so zapletene, težavne oziroma izpostavljene nenehnemu tehnološkemu in

strokovnemu napredku, zagotovi nadzor zunanjih, nepristranskih in neodvisnih opazovalcev oziroma nadzornikov« (Bien Karlovšek in drugi 2006, 4/15).

3.1.7 Kazenske določbe (91. - 103. člen)

Zakon v nadaljevanju vsebuje obširne prekrškovne določbe, ki se nanašajo na pravne osebe, samostojne podjetnike in odgovorne osebe pravnih oseb. S prekrški so sankcionirana posamezna nepravilna aktivna ravnanja in pasivnost organa, ki bi sicer moral opraviti določene aktivnosti, gre za t.i. molk organa. Kot pravi Lampe (2004, 302) pa kazenske določbe v zvezi z varstvom osebnih podatkov definira tudi Kazenski zakonik, ki inkriminira uporabo osebnih podatkov v nasprotju z ZVOP-1.

Sankcije oziroma kazni za prekrške, do katerih pride v primeru kršitve določb zakona so določene v obliki glob, pri čemer višina globe variira glede na težo prekrška in glede na subjekt, ki je za prekršek odgovoren. Najvišja kazen je predpisana za nekatere hujše prekrške pravnih oseb in samostojnih podjetnikov, če zagrešijo nekatere splošne kršitve določb ZVOP-1 kot so na primer obdelovanje osebnih podatkov brez ustrezne pravne podlage, nezakonita uporaba istega povezovalnega znaka, nepopolno vodenje kataloga osebnih podatkov in zbiranje podatkov za nedoločene ali nezakonite namene (Bien Karlovšek in drugi 2006).

3.1.8 Prehodne in končne določbe (104. - 117. člen)

»Prehodne in končne določbe določajo roke za izdajo podzakonskih predpisov, ter kdaj se začnejo uporabljati določbe tega zakona. Zakon določa tudi prenehanje veljavnosti Zakona o varstvu osebnih podatkov iz leta 1999 in posamezne določbe drugih zakonov, spremembe v drugih zakonih in začetek veljavnosti novega zakona ZVOP-1 je tako začel veljati 1. januarja 2005« (Likar 2009, 21).

Poleg Ustave, ZVOP-1, ZInfP in zakonov, ki podrobneje predpisujejo obdelavo osebnih podatkov na posameznem področju, se v Sloveniji pri obdelavi osebnih podatkov neposredno uporabljajo tudi določbe že prej omenjene Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Letno poročilo Informacijskega pooblaščenca 2009, 30).

ZVOP-1 poleg nekaterih pristojnosti pooblaščenca, torej načelno določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Določa tudi, da je na ozemlju Republike Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotovljeno varstvo osebnih podatkov. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo.

4 INFORMACIJSKI POOBLAŠČENEC

Z Zakonom o dostopu do informacij javnega značaja (ZDIJZ) je bil ustanovljen samostojen in neodvisen državni organ, Pooblaščenec za dostop do informacij javnega značaja, ki je začel prvič delovati septembra 2003.

> *Pomembno je, da je bil Pooblaščenec za dostop do informacij javnega značaja po izrecni zakonski določbi samostojen državni organ. Samostojnost Pooblaščenca je bila izkazana na več načinov. Bistveno pa je bilo, da je imel Pooblaščenec za dostop do informacij javnega značaja kot status državnega funkcionarja in da ga je imenoval Državni zbor Republike Slovenije na predlog predsednika Republike Slovenije. Pooblaščenec je imel strokovno službo, ki je bila z zakonom omejena do 15.7.2005 na dva svetovalca. Organizacijsko-administrativne naloge za Pooblaščenca pa je zagotavljalo ministrstvo za informacijsko družbo* (Informacijski pooblaščenec) .

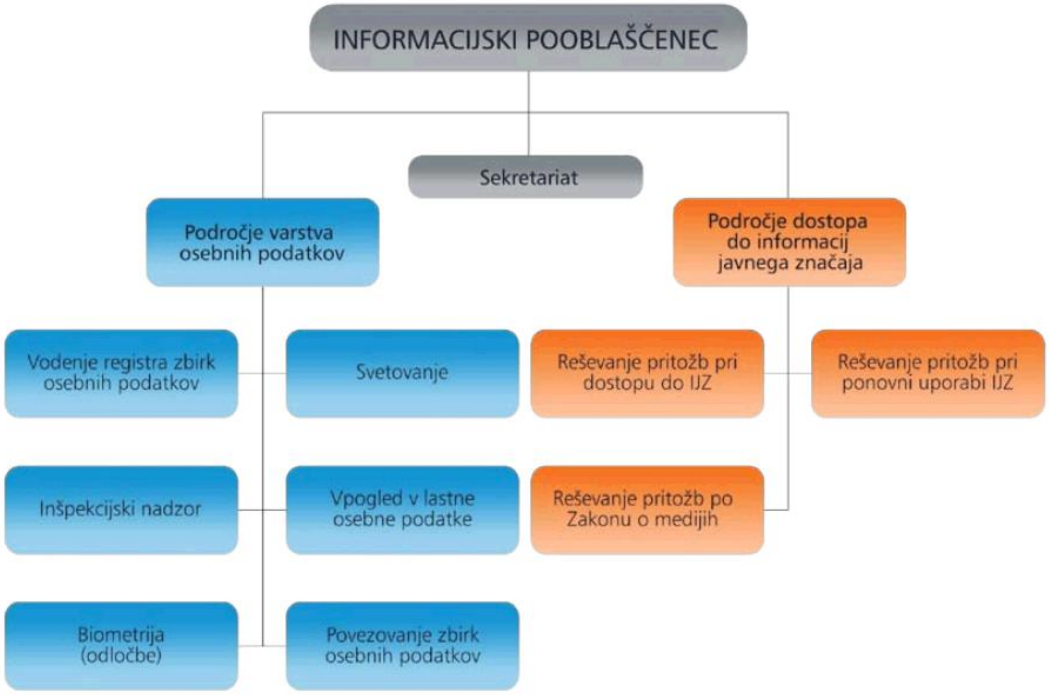
Ko je januarja 2005 stopil v veljavo ZVOP-1, je ta v slovenski pravni red prenesel Direktivo 95/46/ES v pravni red Republike Slovenije. Pred uveljavitvijo ZVOP-1 je bil za varstvo osebnih podatkov pristojen Inšpektorat za varstvo osebnih podatkov, kot organ v sestavi Ministrstva za pravosodje. Inšpektorat je tako bil v razmerju do ministrstva organ prve stopnje. Po Zakonu o informacijskem pooblaščencu (ZInfP), ki je stopil v veljavo decembra 2005, pa sta se Inšpektorat za varstvo osebnih podatkov in Pooblaščenec za dostop do informacij javnega značaja združila.

S sprejemom ZInfP je bila spoštovana določba ZVOP-1, da s 1. januarjem 2006 začne delovati državni nadzorni organ za varstvo osebnih podatkov, ki ima položaj samostojnega

državnega organa, ter določba Direktive, ki predvideva ustanovitev takega organa. Informacijski pooblaščenec je samostojen in obenem tudi neodvisen državni organ.

> *Z ustanovitvijo Informacijskega pooblaščenca so prenehale veljati tudi tiste določbe ZVOP-1, ki bi omogočale sprožitev upravnega spora v primerih, ko bi odločitev Državnega nadzornega organa za varstvo osebnih podatkov po oceni Pooblaščenca za dostop do informacij javnega značaja kršila dostop do informacij javnega značaja in obratno, če bi Državni nadzorni organ ocenil, da je Pooblaščenec za dostop do informacij javnega značaja kršil varstvo osebnih podatkov (Informacijski pooblaščenec 2011).*

Slika 4.1: Organigram Informacijskega pooblaščenca



Vir: Letno poročilo Informacijskega pooblaščenca (2010, 4).

ZInfP prestavlja krovni zakon, ki povezuje ZDIJZ in ZVOP-1 v celoto. Pregled pristojnosti iz ZInfP hitro pokaže, da ima Informacijski pooblaščenec številne pristojnosti, ki so urejene v vseh treh navedenih zakonih. V ZInfP so sicer v splošni obliki naštete pristojnosti Informacijskega pooblaščenca, ki se nanašajo na obe pravni področji, na dostop do informacij javnega značaja in na nadzor nad varstvom osebnih podatkov. Informacijski pooblaščenec ja torej pristojen za inšpekcijski nadzor nad izvajanjem vseh predpisov, ki urejajo varstvo osebnih podatkov, zato ni potrebno posebej urediti inšpekcijskega nadzora nad osebnimi

podatki na kateremkoli področju. Po navedbah Pirc Musarjeve (2006, 7) lahko poleg Informacijskega pooblaščenca inšpekcijski nadzor izvajajo le državni nadzorniki za varstvo osebnih podatkov pri informacijskem pooblaščencu. Nadzornik ima po določbi 53. člena ZVOP-1 pooblastilo, da vpogleda v dokumentacijo, ki se kakorkoli nanaša na obdelavo osebnih podatkov in to ne glede na njeno zaupnost ali tajnost. Šele nadzornikova seznanitev z obdelovanimi osebnimi podatki omogoča izvrševanje varstva osebnih podatkov, saj se le tako neposredno preveri in ugotovi ali je bilo kršeno varstvo osebnih podatkov.

4.1 Pristojnosti Informacijskega pooblaščenca

Med pristojnosti Informacijskega pooblaščenca na podlagi ZVOP-1 sodijo:

1. izvrševanje inšpekcijskega nadzora nad izvajanjem določb ZVOP-1 (obravnava prijave, pritožbe, sporočila in druge vloge, v katerih je izražen sum kršitve zakona);

2. odrejanje inšpekcijskih ukrepov kot so prepoved obdelave osebnih podatkov, anonimiziranje, blokiranje, brisanje ali uničenje osebnih podatkov kadar ugotovi, da se obdelujejo v nasprotju z zakonom;

3. odrejanje drugih ukrepov inšpekcijskega nadzora v skladu z Zakonom o inšpekcijskem nadzoru in Zakonom o splošnem upravnem postopku;

4. opravljanje preventivnih inšpekcijskih nadzorov pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja;

5. vodenje in vzdrževanje registra zbirk osebnih podatkov in skrb, da je register ažuren ter javno dostopen prek svetovnega spleta;

6. omogočanje vpogleda in prepisa podatkov iz registra zbirk osebnih podatkov, praviloma isti dan, najpozneje pa v osmih dneh;

7. vodenje postopkov o prekrških s področja varstva osebnih podatkov;

8. podajanje kazenskih ovadb oziroma izvajanje postopkov v skladu z zakonom, ki ureja prekrške, če pri inšpekcijskem nadzoru ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška;

9. odločanje o ugovoru posameznika glede obdelave osebnih podatkov;

10. izdajanje odločb o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (ZVOP-1, 63. čl.);

11. vodenje postopkov ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacij (ZVOP-1, 64. čl.);

12. vodenje seznama tretjih držav, za katere je ugotovil, da imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov, ali da te nimajo zagotovljene; če je ugotovljeno, da tretja država le delno zagotavlja ustrezno raven varstva osebnih podatkov, je v seznamu navedeno tudi, v katerem delu je ustrezna raven zagotovljena;

13. vodenje upravnih postopkov za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo;

14. vodenje upravnih postopkov za izdajo dovoljenj za povezovanje javnih evidenc in javnih knjig, kadar katera od zbirk osebnih podatkov, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke ali pa je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (na primer EMŠO ali davčna številka);

15. vodenje upravnih postopkov za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba izvajanja biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1;

16. sodelovanje z državnimi organi, pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov, mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji ter drugimi organi in organizacijami glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov;

17. dajanje in objavljanje predhodnih mnenj državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;

18. dajanje in objavljanje neobveznih mnenj o skladnosti kodeksov poklicne etike, splošnih pogojih poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;

19. pripravljanje, dajanje in objavljanje neobveznih navodil in priporočil glede varstva osebnih podatkov na posameznem področju;

20. dajanje izjav za javnost o opravljanih nadzorih in pripravljanje letnih poročil o svojem delu v preteklih letih;

21. odločanje o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugodi zahtevi posameznika glede pravice posameznika do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov (pristojnost je določena v Zakonu o informacijskem pooblaščencu);

22. sodelovanje v delovnih skupinah za varstvo osebnih podatkov, oblikovanih znotraj EU, ki združujejo neodvisne institucije za varstvo osebnih podatkov držav članic (v Delovni skupini po členu 29 Direktive 95/46/EC in v nadzornih organih, ki se ukvarjajo z nadzorom obdelave osebnih podatkov v Schengenskem informacijskem sistemu, v informacijskem sistemu za carino, v okviru Europola ter v skupini za nadzor Eurodaca).

Poleg določb ZInfP in ZVOP-1, Informacijskega pooblaščenca pri delu zavezujejo tudi določbe številnih drugih zakonov, kot najpomembnejše naj navedem Zakon o elektronskih komunikacijah, Zakon o pacientovih pravicah, Zakon o osebni izkaznici, Zakon o potnih listinah, Zakon o bančništvu in Konvencija o izvajanju Schengenskega sporazuma, obenem pa vsakodnevno izvršuje tudi zakone kot so Zakon o prekrških, Zakon o inšpekcijskem nadzoru, Zakon o tajnih podatkih, Zakon o splošnem upravnem postopku in druge.

5 ANALIZA LETNIH POROČIL

Ker je ena izmed pristojnosti Informacijskega pooblaščenca tudi izdajanje letnih poročil, se bom v tem delu diplomskega dela osredotočila na analizo Letnih poročil Informacijskega pooblaščenca med leti 2006 in 2010. Letna poročila so v poglavju Delo na področju varstva osebnih podatkov, razdeljena na več podpoglavij, in sicer na inšpekcijski nadzor, na storjene prekrške, na dajanje pisnih mnenj in pojasnil, na podpoglavje o dopustnosti izvajanja biometrijskih ukrepov, na izdajanje dovoljenj za povezovanje javnih evidenc ter na podpoglavje o seznanitvi z lastnimi osebnimi podatki. Glede na zastavljena raziskovalna vprašanja in hipotezo, sem se pri analizi osredotočila na inšpekcijski nadzor, na število storjenih prekrškov zaradi kršitev določb ZVOP-1, ter na število zaprosil za mnenja.

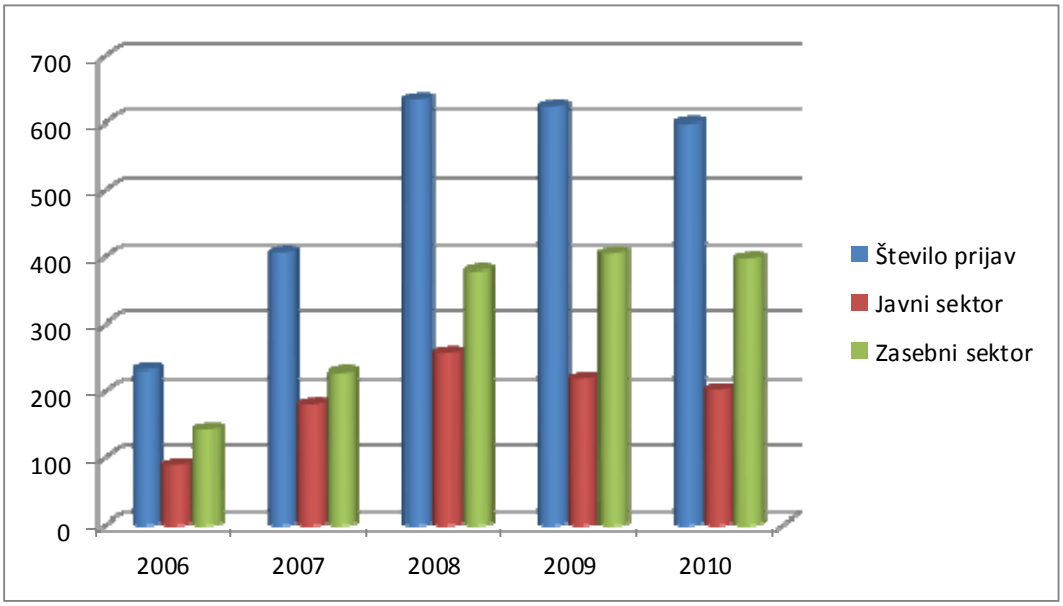
Neposredni inšpekcijski nadzor nad izvajanjem predpisov s področja varstva osebnih podatkov obsega nadzor zakonitosti obdelave osebnih podatkov; nadzor ustreznosti ukrepov za zavarovanje osebnih podatkov ter izvajanja postopkov in ukrepov za zavarovanje osebnih podatkov po 24. in 25. členu ZVOP-1; nadzor nad izvajanjem določb zakona, ki urejajo katalog zbirke osebnih podatkov, register zbirk osebnih podatkov in evidentiranje posredovanja osebnih podatkov posameznim uporabnikom osebnih podatkov; ter nadzor nad izvajanjem določb zakona v zvezi z iznosom osebnih podatkov v tretjo državo in njihovim posredovanjem tujim uporabnikom osebnih podatkov (Letno poročilo Informacijskega pooblaščenca 2010, 30).

5.1 Inšpekcijski nadzor

Po navedbah letnih poročil je Informacijski pooblaščenec leta 2010 zaradi suma kršitev določb ZVOP-1 vodil 599 zadev, 202 v javnem in 397 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je prejel 176 prijav, 26 postopkov pa je uvedel po uradni dolžnosti, medtem ko je zoper zasebni sektor prejel 367 prijav, 30 postopkov pa je uvedel po uradni dolžnosti. V letu 2009 je pooblaščenec vodil 624 zadev, 219 v javnem in 405 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je prejel 165 prijav, 54 postopkov pa je uvedel po uradni dolžnosti, medtem ko je zoper zasebni sektor prejel 322 prijav, 73 postopkov je uvedel po uradni dolžnosti.

Leta 2008 je Informacijski pooblaščenec vodil največ zadev in sicer 635, od tega 256 v javnem in 379 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je tega leta prejel 192 prijav, 64 postopkov je uvedel po uradni dolžnosti, medtem ko je zoper zasebni sektor prejel 310 prijav, 69 pa jih je uvedel po uradni dolžnosti. Leta 2007 je bilo vodenih 406 postopkov zaradi suma kršitev določb ZVOP-1, 179 v javnem in 227 v zasebnem sektorju. Zoper pravne osebe javnega sektorja je omenjenega leta prejel 139 prijav, 40 postopkov pa je bilo uvedenih po uradni dolžnosti. Zoper pravne osebe zasebnega sektorja pa je bilo uvedenih 197 postopkov zaradi prijav in 30 po uradni dolžnosti.

Slika 5.1: Število prijav zaradi suma kršitev določb ZVOP-1 med letoma 2006 in 2010



Vir: prirejeno po Letnih poročilih Informacijskega pooblaščenca (2010, 32).

Za leto 2006 poznamo samo podatek o številu prijav in sicer je bilo teh v javnem sektorju 88, v zasebnem pa 143, skupaj torej 231. Ugotovimo lahko, da je število postopkov pri Informacijskem pooblaščencu skokovito naraslo med leti 2006 in 2008, nato pa se je število postopkov, med leti 2008 in 2010, »ustalilo« tako da se obdržalo na približno enaki ravni oziroma je začelo rahlo padati.

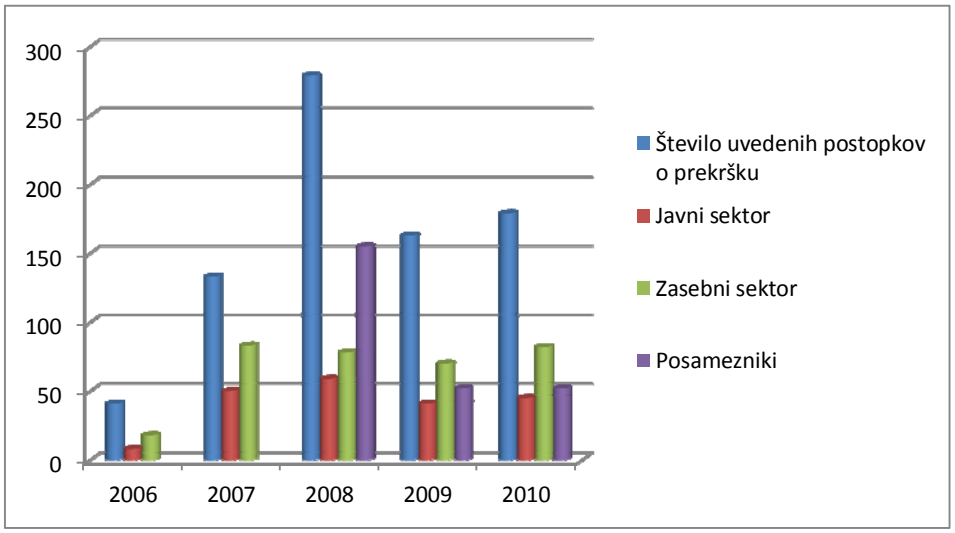
5.2 Storjeni prekrški

Drugo podpoglavje se nanaša na postopke o prekršku, ki se vodijo v skladu z Zakonom o prekrških. Za ugotovljeni prekršek lahko prekrškovni organ izreče opozorilo, če je prekršek neznaten in če pooblaščena uradna oseba oceni, da je glede na pomen dejanja opozorilo zadosten ukrep, če pa je storjen hujši prekršek, pa prekrškovni organ izda odločbo o prekršku, s katero kršitelju izreče sankcijo.

V letu 2010 je bilo uvedenih 179 postopkov o prekršku, 45 zoper javni sektor, 82 zoper zasebni in 52 zoper posameznike. Leta 2009 je bilo postopkov o prekršku zoper posameznike enako, zoper javni sektor 41 in zoper zasebni sektor 70. V letu 2008 je bilo uvedenih največ, kar 279 postopkov o prekršku, največ zoper posameznike in sicer kar 155, sledil je zasebni

sektor s 78 in javni z 59 postopki o prekršku. Za leti 2007 in 2006 nimamo popolnih podatkov, saj nimamo informacij o postopkih zoper posameznike.

Slika 5.2: Število uvedenih postopkov o prekršku med letoma 2006 in 2010

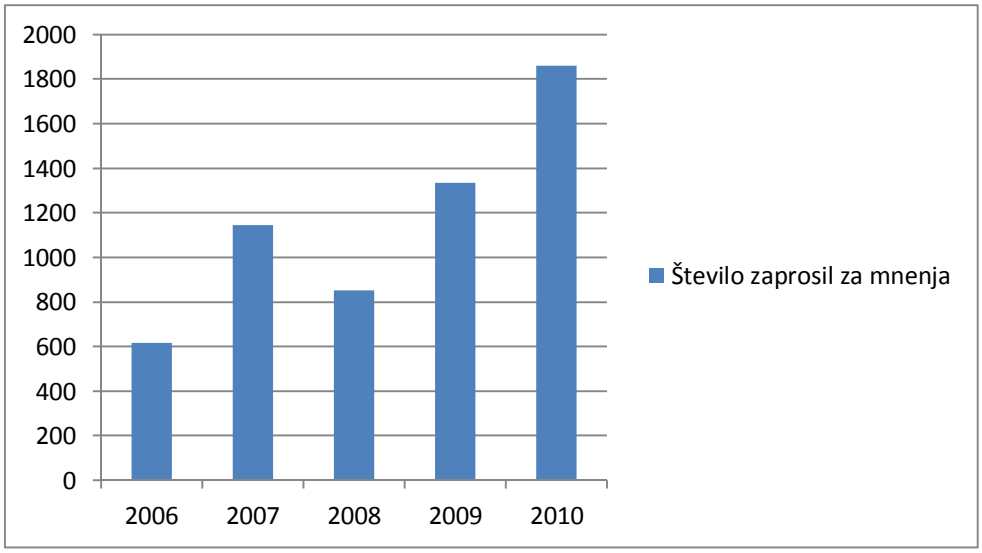


Vir: prirejeno po Letnih poročilih Informacijskega pooblaščenca (2010, 33).

5.3 Dajanje pisnih mnenj in pojasnil

Zadnje podpoglavje, ki sem ga natančneje pregledala, je bilo dajanje pisnih mnenj in pojasnil. Neposredno pravno podlago za dajanje neobveznih mnenj, stališč, navodil in priporočil s področja varstva osebnih podatkov predstavlja 49. člen ZVOP-1. Po navedbah Letnih poročil Informacijskega pooblaščenca so zaprosila za mnenja in pojasnila vsako leto vsebinsko zahtevnejša, kar lahko obrazložimo z dejstvom, da je javnost vedno bolj seznanjena s pravicami, ki so posamezniku zagotovljene v okviru varstva osebnih podatkov. Kot lahko opazimo je bilo najmanjše število zaprosil za mnenja leta 2006, ko je to število znašalo 616, sledi leto 2008, saj je bilo takrat teh zaprosil 853. Leta 2007 je bilo zaprosil za mnenja in pojasnila 1144, leta 2009 jih je bilo 1334, daleč največ pa jih je bilo v preteklem letu, in sicer 1859.

Slika 5.3: Število zaprosil za mnenja med letoma 2006 in 2010



Vir: prirejeno po Letnih poročilih Informacijskega pooblaščenca (2010, 35).

Ugotovimo lahko, da je Informacijski pooblaščenec, pri svojem delu na področju varstva osebnih podatkov, zaznal zlasti porast števila vprašanj, ki jih v zvezi z varstvom osebnih podatkov nanj naslavljajo fizične in pravne osebe ter rahel porast števila pritožb zaradi zavrnitve zahteve po seznanitvi z lastnimi podatki, medtem ko število inšpekcijskih zadev in število prekrškovnih zadev ostaja na podobnem nivoju že zadnja tri leta.

6 ZAKLJUČEK

Dva izmed najpomembnejših dokumentov na področju varstva osebnih podatkov sta obravnavana Direktiva 95/46/ES in ZVOP-1, dopolnjujejo pa ju še ZInfP, ZDIJZ, Direktiva o zasebnosti elektronskih telekomunikacij ter številni drugi pravni akti. Po podatkih pridobljenih z intervjujema, lahko ugotovimo, da je področje varstva osebnih podatkov v praksi, v okviru delovanja javnega sektorja, dokaj dobro urejeno. Po pregledu letnih poročil Informacijskega pooblaščenca lahko sklepamo, da prihaja do kršitev varstva na področju osebnih podatkov, v večji meri v zasebnem sektorju, kjer je področje dopustnosti obdelovanja osebnih podatkov razširjeno, v primerjavi z javnim sektorjem, kjer se lahko obdelujejo le zakonsko določeni podatki. Kako dobro je varovanje osebnih podatkov v javnem sektorju urejeno, lahko sklepamo tudi na podlagi opravljenih intervjujev s predstavniki javnih ustanov. Tako predstavnik Ministrstva za notranje zadeve, kot tudi predstavnik javnega zdravstvenega

zavoda navajata dejstvo, da morajo vsi zaposleni podpisati poseben dokument s katerim se zavežejo k varovanju osebnih podatkov, prav tako pa ima vsakdo za vpogled v različne evidence, svoje lastno geslo, njegovi vpogledi pa so sledljivi. Največji problem predstavljajo še vedno podatki, ki jih različne ustanove posredujejo dalje v fizični obliki, to so različni dokumenti, ki se na primer predajajo tožilstvu v okviru delovanja Ministrstva za notranje zadeve ali pa izvidi, ki se posredujejo pacientom.

Na področju storjenih oziroma prijavljenih prekrškov, ima ponovno vodilno mesto zasebni sektor, sledijo pa mu posamezniki. Morda bi razlog za to lahko pripisali preširoki definiciji dopustnosti obdelave posameznikovih osebnih podatkov; saj za pravne ali fizične osebe, ki opravljajo javno službo ali dejavnost po zakonu, ki ureja gospodarske družbe, namreč velja, da lahko že neposredno na podlagi ZVOP-1, torej brez izrecne podlage v nekem drugem zakonu ali pisne privolitve posameznika, obdelujejo osebne podatke oseb, s katerimi so v pogodbenem razmerju, vendar le, če gre za osebne podatke, ki jih potrebujejo za izpolnjevanje pogodbenih obveznosti ali uveljavljanje pravic iz pogodbenega razmerja.

Ugotovili smo tudi, da število inšpekcijskih zadev in število prekrškovnih zadev že zadnja tri leta ostaja na približno isti ravni. Število prijav je po ustanovitvi Pooblaščenca najprej skokovito naraščalo, kar lahko po navedbah Tomšiča pripišemo predvsem dvema dejavnikoma. Po eni strani je pooblaščenec v teh letih šele pridobival predvidene kadre (državne nadzornike za varstvo osebnih podatkov), po drugi strani pa je hkrati s tem naraščala tudi splošna ozaveščenost o zakonodaji in pomenu varstva osebnih podatkov. Ustalitev števila prijav po oceni namestnika Informacijske pooblaščenke, v grobem odraža visok nivo obveščenosti splošne javnosti, posameznikov in zavezancev glede zahtev na področju varstva osebnih podatkov. Vsekakor bi bilo manjše število prijav v bodoče spodbudno, če izhajamo iz predpostavke, da pomeni manj prijav tudi manj kršitev, vendar pa je na tem področju težko podajati ocene za prihodnost, saj je varstvo osebnih podatkov zelo tesno vezano na hiter razvoj informacijsko-komunikacijskih tehnologij, kjer se spremembe dogajajo zelo hitro. Nekatere spremembe tako lahko povzročijo povečan pripad novih prijav.

Z vidika ZVOP-1 je na področju varstva osebnih podatkov vsekakor kar nekaj možnosti za izboljšave. Informacijski pooblaščenec je predlog sprememb ZVOP-1 že leta 2009 posredoval Ministrstvu za pravosodje, a do sprememb še ni prišlo. Po navedbah Tomšiča gre večinoma za spremembe, ki so povezane s praktičnim izvajanjem zakona v praksi glede na konkretne izkušnje Informacijskega pooblaščenca, med zaželenimi spremembami pa lahko omenimo

spremembo kriterijev glede izjem v 7. členu ZVOP-1 (predvsem trenutna meja 50 zaposlenih), možnost izrekanja sankcij v razponu, natančnejše dikcije pri ureditvi videonadzora in konkretna ureditve glede izvajanja videonadzora na javnih površinah, bolj sistematična ureditev zavarovanja osebnih podatkov pri prenosu prek elektronskih omrežij.

Na drugi strani imamo evropsko zakonodajo, ki je že sedaj med najbolj strogimi na svetu, vendar pa je še vedno obstaja nekaj možnosti za izboljšave, kot je potreba po večji harmonizaciji. Eden ključnih izzivov je, kako zagotoviti spoštovanje evropske ureditve v globaliziranem in povezanem svetu, kjer so največji zbiralci osebnih podatkov (npr. ponudniki spletnih družabnih omrežij, spletnih iskalnikov, računalništva v oblaku ipd.) izven jurisdikcije EU, svoje storitve pa ponujajo evropskih državljanom. Med potrebne spremembe evropske zakonodaje bi po navedbah Tomšiča uvrstili tudi nujo po spremembi pristopa k t.i. politikam zasebnosti na internetu, ki so se izkazale kot popolnoma neučinkovit mehanizem, saj so običajno pisane v uporabnikom nerazumljivem jeziku, ne ponujajo zahtevanih informacij in v splošnem ne dosegajo svojega namena. Eden od mehanizmov, ki je deležen resnega razmisleka, je uvedba obveznega poročanja o varnostnih incidentih (t.i. mandatory breach notification), ki od upravljavcev osebnih podatkov, ki izgubijo osebne podatke svojih strank oziroma so ti podatki ogroženi zaradi varnostnega incidenta, zahteva, da o tem obvestijo svoje stranke. Gre za sankcijo, ki ima precej večjo težo, kot je recimo zagrožena globa v marsikateri državi.

Glede povečevanja transparentnosti obdelave osebnih podatkov bo v bližnji prihodnosti Komisija preučila možnosti uvedbe strožjih obveznosti za obveščanje posameznika in standardnih obrazcev za pisanje izjav o zasebnosti, opredelila se bo do različnih načinov podajanja privolitve. »Naslednje, kar Komisijo skrbi predvsem v luči socialnih omrežij, je povečanje nadzora posameznika nad obdelovanjem svojih podatkov in pravica do biti pozabljen. To je pravica posameznikov, da se njihovi podatki ne obdelujejo več, ko niso več potrebni za prvotni namen. V novi evropski strategiji bo tako še večji poudarek na akcijah dvigovanja zavedanja in učinkovitejšega zagotavljanja pravic ter preganjanja kršiteljev« (Burnik 2011, 18). V tej luči velja omeniti tudi pričakovane spremembe Direktive, pri katerih bo s svojimi mnenji in priporočili sodeloval tudi Informacijski pooblaščenec.

Pri vrednotenju implementacije javne politike varovanja osebnih podatkov, smo preučevali obdobje od leta 2006, ko je bila sprejeta novela ZVOP-1, do leta 2010. Po podatkih pridobljenih v letnih poročilih Informacijskega pooblaščenca lahko trdimo, da je med leti

2006 in 2008 obstajal trend naraščanja zahtev za nadzor nad izvajanjem določb ZVOP-1, med leti 2008 in 2010 pa je ta obstal na približno enaki ravni. Na področju prekrškov bi omenila leto 2008, ko je bilo zabeleženo največje število uvedenih postopkov o prekršku, potem pa je tudi to število v letih 2009 in 2010 upadlo in se ustalilo. Najbolj zanimivo je področje dajanja pisnih mnenj in pojasnil, kjer Informacijski pooblaščenec beleži največji porast, za to področje je torej značilen konstanten trend rasti.

V skladu z napisanim lahko del zastavljene hipoteze, ki govori o naraščanju števila zaprosil za mnenja potrdim, drugi del hipoteze, ki govori o naraščanju inšpekcijskih postopkov pred Informacijskim pooblaščenec pa zavržem, saj je število teh zadnja tri leta približno enako in ne narašča. Sama bi implementacijo ZVOP-1, kljub dokaj velikemu številu suma kršitev določb zakona, označila za uspešno, saj je možno zaznati zmanjšanje števila kršitev in povečanje zaprosil za mnenja. Pomembno pa je izpostaviti, da se sama vsebina ZVOP-1 morda ne prilagaja najbolje vsakodnevnim spremembam in nenehnemu razvoju. V tem pogledu bi bila potrebna torej sprememba ZVOP-1, kar bi v okviru cikla določene javne politike, pomenilo vrnitev v fazo najprej iskanja alternativnih rešitev, potem pa uzakonitve.

7 LITERATURA

1. Bien Karlovšek, Sonja, Miro Cerar, Goran Klemenčič, Rok Lampe, Andrej Tomšič, Nataša Belopavlovič, Majda Zorec – Karlovšek in Boštjan Kežmah. 2006. *Zasebnost in varovanje osebnih podatkov na delovnem mestu : aktualna navodila in obrazci za pravno pravilno ravnanje delodajalcev v odnosu do zasebnosti delavcev in varovanje osebnih podatkov.* Maribor: Založba Forum Media.

2. Bohinc, Rado. 2007. *Pravo evropske unije: temelji pravoznanstva EU za študente družboslovja*. Ljubljana: Fakulteta za družbene vede.

3. Brezovšek, Marjan in Damir Črnčec. 2007. *Demokratična uprava in tajnost podatkov*. Ljubljana: Fakulteta za družbene vede.

4. Burnik, Jelena. 2011. Prihodnost varstva osebnih podatkov v EU. *Pravna praksa* 30 (3): 18 – 19.

5. Celestina, Ivan. 2011. Intervju z avtorico. Ljubljana, 8. september.

6. Cvetko, Aleksej. 1999. *Varovanje zasebnosti v delovnih razmerjih*. Ljubljana: Gospodarski vestni.

7. Čebulj, Janez. 1992. *Varstvo informacijske zasebnosti v Evropi in v Sloveniji*. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.

8. --- in Jurij Žurej. 2005. *Varstvo osebnih podatkov in informacije javnega značaja*. Ljubljana: Nebra.

9. Dunn, William N. 1994. *Public Policy Analysis: An Introduction*. Englewood Cliffs: Prentice Hall.

10. Evropski parlament in Svet. 1995. *Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov*. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Direktive_E_parlamenta_in_ Sveta.pdf (25. avgust 2011).

11. Fink Hafner, Danica. 2007. Znanost »o« javnih politikah in »za« javne politike. V *Uvod v analizo politik: Teorije, koncepti, načela*, ur. Danica Fink Hafner, 9–30. Ljubljana: Fakulteta za družbene vede.

12. Fischer, Frank. 2006. *Evaluating Public Policy*. Mason: Cengage Learning.

13. Grdešić, Ivan. 1995. *Političko odlučivanje*. Zagreb: Alinea.

14. Hočevar, Janez. 2011. Intervju z avtorico. Ljubljana, 10. september.

15. --- 2006. *Osnove analize javnih politika*. Zagreb: Fakultet političkih znanosti.

16. *Informacijski pooblaščenec RS*. Dostopno prek: https://www.ip-rs.si/ (30. avgust 2011).

17. --- 2006. *Letno poročilo Informacijskega pooblaščenca za leto 2006.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/letna_ porocila_2006.pdf (25. julij 2011).

18. --- 2007. *Letno poročilo Informacijskega pooblaščenca za leto 2007.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2007.pdf (25. julij 2011).

19. --- 2008. *Letno poročilo Informacijskega pooblaščenca za leto 2008.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno-porocilo-2008.pdf (25. julij 2011).

20. --- 2009. *Letno poročilo Informacijskega pooblaščenca za leto 2009.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2009-net.pdf (25. julij 2011).

21. --- 2010. *Letno poročilo Informacijskega pooblaščenca za leto 2010.* Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2010_net.pdf (25. julij 2011).

22. Kaučič, Igor in Franc Grad. 2003. *Ustavna ureditev Slovenije*. Ljubljana: GV Založba.

23. Kotnik Šumah, Kristina. 2006. Neposredna uporabljivost prava EU in dostop do informacij javnega značaja. *Pravna praksa* 25 (27): 9 – 10.

24. Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Ljubljana: Fakulteta za družbene vede.

25. Kustec Lipicer, Simona. 2007. *Cena uspeha, evalvacijska analiza javne politike boja proti dopingu v vrhunskem športu v Sloveniji.* Ljubljana: Fakulteta za družbene vede.

26. Lajh, Damjan. 2007. Izvajanje javnih politik. V *Uvod v analizo politik: Teorije, koncepti, načela*, ur. Danica Fink Hafner, 155–174. Ljubljana: Fakulteta za družbene vede.

27. Lampe, Rok. 2004. *Sistem pravice do zasebnosti*. Ljubljana: Bonex.

28. Likar, Simon. 2009. *Varstvo osebnih podatkov v policiji*. Ljubljana: Fakulteta za upravo.

29. Maychrzak, Ann. 1984. *Methods for policy research*. Newbury Park, London, New Delhi: Sage.

30. Pirc Musar, Nataša. 2006. Neodvisni nadzor in varstvo osebnih podatkov. *Pravna praksa* 25 (35): 6 – 10.

31. Rossi, Peter H., Mark W. Lipsey in Howard E. Freeman. 2003. *Evaluation: A Systematic Approach. Seventh Edition*. Thousand Oaks, London, New Delhi: Sage Publication.

32. Tomšič, Andrej. 2011. Intervju z avtorico. Ljubljana, 19. september.

33. *Ustava Republike Slovenije.* 1991. Ur. l. RS 33/91. Dostopno prek: http://www.dz-rs.si/index.php?id=150&docid=28&showdoc=1 (25. avgust 2011).

34. *Ustavni zakon o spremembah prvega poglavja ter 47. in 68. člena Ustave Republike Slovenije*. Ur. l. RS 4/2003. Dostopno prek: http://www.dz-rs.si/index.php?id=150&docid=4&showdoc=1 (25. avgust 2011)

35. Vedung, Evert. 2005. *Public policy and Program Evaluation*. London: Transaction Publishers.

36. Weiss, Carol H. 1998. *Evaluation. Methods for studying programs and policies*. New York: Prentice hall, Upper Sadle River.

37. *Zakon o dostopu do informacij javnega značaja* (ZDIJZ-UPB2). Ur. l. RS 51/2006. Dostopno prek: http://www.uradni-list.si/1/content?id=73398&part=&highlight=zakon+o+dostopu (28. julij 2011).

38. *Zakon o informacijskem pooblaščencu* (ZInfP). Ur. l. RS 113/2005. Dostopno prek: http://www.uradni-list.si/1/content?id=59461&part=&highlight=zakon+o+informacijskem+pooblaščencu (28. julij 2011).

39. *Zakon o varstvu osebnih podatkov* (ZVOP-1-UPB1). Ur. l. RS 94/2007. Dostopno prek: http://www.uradni-list.si/1/content?id=82668&part=&highlight=zvop (15. julij 2011).

PRILOGE

PRILOGA A: Intervju z mag. Ivanom Celestino, vodjo sektorja za analize, policijsko pravo in sistemsko normativno dejavnost pri Ministrstvu za notranje zadeve (MNZ)

1. Po podatkih Letnega poročila Informacijskega pooblaščenca za leto 2010 je bilo vloženih prijav zaradi suma kršitev določb ZVOP - 1 57, zoper državne organe, ministrstva in organe v njihovi sestavi. Ker imate tudi sami pri delu omogočen dostop do »občutljivih« podatkov me zanima kako skrbite za varstvo osebnih podatkov?

Odgovor na to vprašanje je zelo kompleksen. Informacijska pooblaščenka izdaja odločbe tudi v drugih primerih, na primer dostop do informacij javnega značaja. Redke so tiste odločbe, ki bi urejale kršitve varstva osebnih podatkov. Vsaj za MNZ lahko to trdim. Je pa res, da informacijska pooblaščenka zel natančno spremlja razvoj tega področja v tujini in poskuša kar se da hitro implementirati »dobre rešitve«.

Sedaj pa k odgovoru. MNZ ima zelo strogo urejeno poslovanje s podatki (ne samo z osebnimi). Dostopi s sistemi gesel, naknadno preverjanje vstopanj v baze podatkov, označevanje posebnih območij kjer se hranijo podatki, obvezno izklapljanje računalnikov in zaklepanje pisarn so tisti ukrepi, ki sodijo v osnovo poslovanja. Hkrati smo zaposleni podpisali še posebno izjavo s katero smo se zavezali k varovanju vseh podatkov (osebnih, tajnih in varovanih podatkov). V pogodbah o zaposlitvi je tovrstna kršitev zelo strogo sankcionirana in praviloma predstavlja prekinitev delovnega razmerja. Naj za ilustracijo povem, da že rokovniki predstavljajo interno gradivo in ga ni mogoče kar tako odvreči v koš za papir.

2. Ali menite, da so podatki, ki se nahajajo v evidenci kaznivih dejanj, evidenci pridržanih, evidenci kršiteljev in prekrškov itd. ustrezno zavarovani? Je kdaj že prišlo do zlorab pri dostopu omenjenih evidenc?

Evidence, katere omenjate, so vzpostavljene na podlagi Zakona o policiji. Če ni zakonske podlage, potem ne more biti evidence, seznama ali kaj podobnega. To je pogoj. Gre na eni strani za papirno evidenco v posameznih enotah ter hkrati za centralno računalniško evidenco. Tovrstno gradivo ima oznako interno. Vstop v računalniško evidenco se beleži, saj je omogočen zgolj s posebnim individualnim geslom. V policiji obstaja praksa, da naključno

preverijo t.i. »žurnal« posameznega delavca iz katerega je razvidno kdaj je vstopal v evidenco in kaj je gledal ter pri takem delavcu naknadno preverijo zakonsko upravičenost vpogleda. Vsak delavec mora pojasniti razlog vpogleda, sicer je storil disciplinsko kršitev, če pa je podatke posredoval tretjemu pa je lahko storil tudi kaznivo dejanje.

Evidence, katere ste navedli so tiste vrste, kjer se podatki posredujejo pristojnim sodiščem – torej zunanjim institucijam, zato je večja možnost zlorab. Seveda pa so tovrstne zlorabe mogoče tudi znotraj MNZ, vendar pa so ti primeri sorazmerno redki, predvsem pa zelo strogo sankcionirani.

3. Kako ocenjujete varstvo osebnih podatkov v Sloveniji? Ali menite, da bi bilo potrebno področje varstva osebnih podatkov zakonsko natančneje urediti?

Kot sem že omenil, gre za pravno področje, ki se nenehno razvija. Temu poskuša veljavna ureditev slediti, čeprav včasih ne ravno hitro in učinkovito. Pretirano ščitenje osebnih podatkov je včasih za organe pregona lahko zelo dvorezen meč. Tega se zavedamo vsi. Omejitve pri uporabi številnih javnih kamer, zakonsko omejene možnosti hranjenja DNK sledi, relativno hitro brisanje nepotrjenih sumov storitve kaznivih dejanj so takšni primeri. Na drugi strani pa se je potrebno zavedati, da gre za hude posege v človekove pravice in temeljne svoboščine, ki morajo biti natančno regulirane. Hkrati pa smo ljudje, ki z pretiranim posredovanjem podatkov, nekontrolirano omogočimo drugim, da do potankosti spoznajo naše življenje, pogosto tisti, ki prispevamo k zlorabam. Ampak takrat je že prepozno. Facebook in podobna omrežja so tipičen primer.

Na koncu naj še povem, da ni zgolj Zakon o varstvu osebnih podatkov tisti, ki ščiti osebne podatke. Ravno sedaj je v Državnem zboru nov Zakon o nalogah in pooblastilih policije, ki ima vrsto takšnih določb (bistveno več kot sedaj veljavni Zakon o policiji).

PRILOGA B: Intervju z g. Janezom Hočevarjem, odgovornim za informacijsko varnost na Zavodu za transfuzijsko medicino (ZTM)

1. Ker imate pri delu omogočen dostop do »občutljivih« podatkov (podatki o pacientih) me zanima kako skrbite za varstvo osebnih podatkov?

Na ZTM imamo sprejet Pravilnik o varstvu osebnih podatkov, trenutno pa uvajamo tudi Sistem upravljanja z varnostjo informacij (SUVI) po standardu ISO 27000. Ta mednarodni standard je bil pripravljen za zagotovitev modela vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema za upravljanje varovanja informacij v organizaciji. Poleg tega imamo uvedene tudi določene tehnične in organizacijske ukrepe, ki zagotavljajo informacijsko varnost.

Dostop do informacijskih sistemov je zaščiten s sistemom gesel, šiframi za naknadno preverjanje vstopanj v baze podatkov, fizično zaščito območij kjer se hranijo podatki, zaklepanjem prostorov in videonadzorom dostopov. Hkrati smo zaposleni podpisali še posebno izjavo s katero smo se zavezali k varovanju občutljivih osebnih podatkov. V pogodbah o zaposlitvi je vključena posebna klavzula, ki zavezuje zaposlene k varovanju osebnih podatkov.

Kljub temu je za zagotavljanje informacijske varnosti potrebno storiti še marsikaj, področje pa je potrebno tudi stalno spremljati, uvajati potrebne ukrepe in spremljati njihovo učinkovitost. Zavzemamo se za sistematičen pristop k reševanju problemov, kar zagotavljajo standardi. Zavedamo se namreč, da večja informacijska varnost pomeni tudi izboljšanje kvalitete storitev zavoda.

2. Ali menite, da so podatki, ki se nahajajo v evidenci ustrezno zavarovani? Je kdaj že prišlo do zlorab pri dostopu omenjenih evidenc?

Zbirke podatkov so vedno vzpostavljene na podlagi zakonodaje. Če ni zakonske podlage potem ne more biti zbirke podatkov. Gre na eni strani za dokumente v papirni obliki ter hkrati za centralno računalniško evidenco.

V informacijskem sistemu se vodi dnevnik vstopov v računalniške evidence (t.i. »sledljivost«). Pravice za delo s podatki (vnos, spreminjanje, vpogledi ipd.) so usklajene oziroma omejene s potrebami zaposlenih glede na njihove naloge in zadolžitve v procesu dela. Do večjih zlorab do sedaj še ni prišlo, zato menimo da so podatki ustrezno varovani, ker

pa je stopnja ogroženosti vse višja, bo potrebno sprejeti dodatne ukrepe (v skladu s standardom ISO 27000). Večji problem predstavlja papirna dokumentaciji, ki je dostopna vsakemu zaposlenemu, ki vstopi v prostore kjer se hranijo.

3. Kako ocenjujete varstvo osebnih podatkov v Sloveniji? Ali menite, da bi bilo potrebno področje varstva osebnih podatkov zakonsko natančneje urediti?

Nekatere organizacije imajo zavedanje o problemu že dovolj visoko oziroma so že dosegle visoko stopnjo zrelosti. Uvedenih imajo dovolj tehničnih in organizacijskih ukrepov, druge pa ne. Zelo pomembna je med drugim tudi »kultura« ki jo goji organizacija. Skrb za informacijsko varnost mora postati del vsakdana zaposlenih.

Stanje bi bilo potrebno urediti z uvajanjem standardov, ki urejajo področje varovanja podatkov (ISO 27000), kar naj bi postalo zakonsko obvezno.

PRILOGA C: Intervju z mag. Andrejem Tomšičem, namestnikom Informacijske pooblaščenke.

1. Kot je razvidno iz letnih poročil Informacijskega pooblaščenca, število prijav zaradi suma kršitev določb ZVOP-1 zadnja tri leta (2008, 2009 in 2010) ostaja na isti ravni. Ali menite da se bo ta trend nadaljeval oziroma kako bi komentirali število prijav?

Število prijav je po ustanovitvi Pooblaščenca najprej skokovito naraščalo, kar lahko pripišemo predvsem dvema dejavnikoma. Po eni strani je pooblaščenec v teh letih šele pridobival predvidene kadre (državne nadzornike za varstvo osebnih podatkov), po drugi strani pa je hkrati s tem rastla tudi splošna ozaveščenost o zakonodaji in pomenu varstva osebnih podatkov. Ustalitev števila prijav po moji oceni v grobem odraža visok nivo obveščenosti splošne javnosti, posameznikov in zavezancev glede zahtev na področju varstva osebnih podatkov. Vsekakor bi bilo manjše število prijav v bodoče spodbudno, če izhajamo iz predpostavke, da pomeni manj prijav tudi manj kršitev, vendar pa je na tem področju težko podajati ocene za prihodnost, saj je varstvo osebnih podatkov zelo tesno vezano na hiter razvoj informacijsko-komunikacijskih tehnologij, kjer se spremembe dogajajo zelo hitro. Nekatere spremembe lahko povzročijo povečan pripad novih prijav.

2. Menite, da bi bilo potrebno področje varstva osebnih podatkov zakonsko natančneje urediti?

Z vidika ZVOP-1 je vsekakor kar nekaj možnosti za izboljšave. Informacijski pooblaščenec je predlog sprememb ZVOP-1 že leta 2009 posredoval Ministrstvu za pravosodje, a do sprememb že ni prišlo. Večino gre za spremembe, ki so povezane s praktičnim izvajanjem zakona v praksi glede na konkretne izkušnje Informacijskega pooblaščenca, med zaželenimi spremembami pa lahko omenim spremembo kriterijev glede izjem v 7. členu ZVOP-1 (predvsem trenutna meja 50 zaposlenih), možnost izrekanja sankcij v razponu, natančnejše dikcije pri ureditvi videonadzora in konkretna ureditve glede izvajanja videonadzora na javnih površinah, bolj sistematična ureditev zavarovanja osebnih podatkov pri prenosu prek elektronskih omrežij (14. člen ZVOP-1) itd.

Z vidika Direktive se vsekakor kaže nekaj perečih težav, zlasti težave pri doseganju harmonizacije ravni varstva osebnih podatkov po EU. Primer Google Street View je lepo

pokazal, kako različne so nacionalne ureditve po posameznih članicah EU, čeprav naj bi izhajale iz iste direktive. Prav gotovo je treba poiskati nove mehanizme za večje sodelovanje nadzornih organov v državah članicah ter poenoteno sankcioniranje. Potrebne spremembe se kažejo tudi na področjih obdelave občutljivih osebnih podatkov, kjer je govora o večjem upoštevanju konteksta obdelave osebnih podatkov in ne zgolj fokusiranja na kategorijo podatkov kot tako. Spremembe so prav gotovo potrebne tudi na področju notifikacije, saj se kaže mehanizem centralnih registrov zbirk osebnih podatkov kot relativno neučinkovit. Poseben izziv za spremembe pa bo dohajanje silovitega tehnološkega razvoja, kateremu zakonodaja le stežka sledi (Google in Facebook sta nastala v zadnjih desetih letih).

3. Kako bi ocenili delo WP29 in njihove pristojnosti? S kakšnimi »problemi« se srečuje WP29 pri svojem delovanju?

Delovna skupine WP29 je vsekakor dobrodošel mehanizem za sodelovanje nadzornih organov, se pa kaže, da v nekaterih situacijah – zlasti ko gre za tuje multinacionalke (npr. Google, Facebook, Yahoo, Microsoft ipd.) – nima dovolj močnih orodij, s katerim bi lahko zagotovila spoštovanje svojih mnenj. Večje pristojnosti so tako prav gotovo eden večjih izzivov. Mnenja WP29 so pogosto zelo rigorozna in včasih v praksi težko izvedljiva, vendar je delovni skupini treba priznati načelnost in vztrajanje na stebrih varstva osebnih podatkov. Kot problem se kaže prenizka zastopanost t.i. novih članic v delovnih podskupinah, kjer se dejansko pripravlja vsebina mnenj.

4. Menite, da bi bilo potrebno »zaostriti« evropsko zakonodajo s področja varstva osebnih podatkov?

Evropska zakonodaja je že sedaj med najbolj strogimi na svetu, vendar pa je še vedno nekaj možnosti za izboljšave, kot je že omenjena potreba po večji harmonizaciji. Eden ključnih izzivov je, kako zagotoviti spoštovanje evropske ureditve v globaliziranem in povezanem svetu, kjer so največji zbiralci osebnih podatkov (npr. ponudniki spletnih družabnih omrežij, spletnih iskalnikov, računalništva v oblaku ipd.) izven jurisdikcije EU, svoje storitve pa ponujajo evropskih državljanom. Med potrebne spremembe evropske zakonodaje bi uvrstil nujo po spremembi pristopa k t.i. politikam zasebnosti na internetu, ki so se izkazale kot popolnoma neučinkovit mehanizem, saj so običajno pisane v uporabnikom nerazumljivem jeziku, ne ponujajo zahtevanih informacij in v splošnem ne dosegajo svojega namena.

Eden od mehanizmov, ki je deležen resnega razmisleka, je uvedba obveznega poročanja o varnostnih incidentih (t.i. mandatory breach notification), ki od upravljavcev osebnih podatkov, ki izgubijo osebne podatke svojih strank oziroma so ti podatki ogroženi zaradi varnostnega incidenta, zahteva, da o tem obvestijo svoje stranke. Gre za sankcijo, ki ima precej večjo težo, kot je recimo zagrožena globa v marsikateri državi.