

Številka: 751-02-51/2005 (0106)

Datum: 30.05.2005

**POROČILO**  
**O DELU INŠPEKTORATA ZA VARSTVO OSEBNIH PODATKOV**  
**V LETU 2004**

**Ljubljana, maj 2005**

## VSEBINA

UVOD .....	3
1. <i>KONCEPT VARSTVA OSEBNIH PODATKOV V RS TER SPREMEMBE V LETU 2004</i> .....	4
2. <i>PRISTOJNOST TER ORGANIZIRANOST INŠPEKTORATA ZA VARSTVO OSEBNIH PODATKOV</i> .....	8
2.1. <i>Pristojnosti in dolžnosti Inšpektorata za varstvo osebnih podatkov</i> .....	8
2.2. <i>Pravice in dolžnosti inšpektorja za varstvo osebnih podatkov</i> .....	9
2.3. <i>Organizacija in kadrovska zasedenost Inšpektorata za varstvo osebnih podatkov ter problematika v zvezi s tem</i> .....	10
3. <i>AKTIVNOSTI INŠPEKTORATA V LETU 2004</i> .....	12
3.1. <i>Inšpekcijski nadzor nad izvajanjem določb ZVOP...</i> .....	12
3.2. <i>Ostale aktivnosti inšpektorata na domačem področju</i> .....	15
3.3. <i>Aktivnosti inšpektorata na mednarodnem področju</i> .....	16
4. <i>PREGLED IN OCENA STANJA VARSTVA OSEBNIH PODATKOV NA PODROČJIH, NA KATERIH SE JE V LETU 2004 OPRAVLJAL NADZOR</i> .....	20
4.1. <i>Državna uprava</i> .....	20
4.2. <i>Pravosodje</i> .....	21
4.3. <i>Lokalna samouprava</i> .....	22
4.4. <i>Vzgoja in izobraževanje</i> .....	23
4.5. <i>Zdravstveno varstvo</i> .....	24
4.6. <i>Delovne evidence in varstvo osebnih podatkov zaposlenih</i> .....	29
5. <i>SPLOŠNA OCENA STANJA NA PODROČJU VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI</i> .....	30
5.1. <i>Nepravilnosti v zvezi s katalogi zbirk osebnih podatkov ter registrom zbirk osebnih podatkov</i> .....	30
5.2. <i>Nepravilnosti v zvezi z zavarovanjem osebnih podatkov ter novosti, ki jih prinaša novi ZVOP-1</i> .....	31
5.3. <i>Nepravilnosti in dileme, ki se pojavljajo v zvezi s pogodbeno obdelavo osebnih podatkov</i> .....	33
5.4. <i>Nepravilnosti in vprašanja, ki se pojavljajo v zvezi s posredovanjem osebnih podatkov drugim uporabnikom ter javnosti</i> .....	35
5.5. <i>Obdelava prekomernih in nepotrebnih osebnih podatkov</i> .....	42
6. <i>PRIPOROČILA ZA IZBOLJŠANJE STANJA NA PODROČJU VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI</i> .....	44

## **UVOD**

Zakon o varstvu osebnih podatkov<sup>1</sup>, ki je stopil v veljavo s 1. januarjem 2005, Državnemu nadzornemu organu za varstvo osebnih podatkov v 46. členu nalaga, da najkasneje do 31. maja Državnemu zboru Republike Slovenije posreduje letno poročilo o svojem delu v preteklem letu in ga objavi na svoji spletni strani. Letno poročilo vsebuje podatke o delu državnega nadzornega organa v preteklem letu ter ocene in priporočila s področja varstva osebnih podatkov.

Pričujoče poročilo je zadnje, ki ga je pripravil še Inšpektorat za varstvo osebnih podatkov kot organ v sestavi Ministrstva za pravosodje. Prihodnje leto bo namreč poročilo o delu nadzornega organa za varstvo osebnih podatkov ter ocene in priporočila s področja varstva osebnih podatkov že pripravil Državni nadzorni organ za varstvo osebnih podatkov, ki bo imel status povsem samostojnega in neodvisnega državnega organa. Državni nadzorni organ za varstvo osebnih podatkov bo začel z delom 1. januarja 2006, do takrat pa bo njegove naloge in pristojnosti izvrševal zdajšnji inšpektorat kot organ v sestavi Ministrstva za pravosodje.

V poročilu o delu v letu 2004 je podobno kot v poročilih o delu, ki so bila pripravljena za prejšnja obdobja, navedenih tudi nekaj podrobnejših pojasnil, tolmačenj in priporočil glede vprašanj, ki se v zvezi z varstvom osebnih podatkov najpogosteje pojavljajo v praksi. V tem okviru so pojasnjene tudi nekatere novosti, ki jih uvaja novi Zakon o varstvu osebnih podatkov in jih je potrebno upoštevati od 1. januarja 2005 dalje.

Na inšpektoratu upamo, da bo predloženo poročilo, poleg seznanitve javnosti z delom Inšpektorata za varstvo osebnih podatkov v letu 2004, z navedbo in obrazložitvijo najpogosteje ugotovljenih nepravilnosti ter opisom stanja na posameznih področjih, pripomoglo predvsem k izboljšanju stanja na področju varstva osebnih podatkov v Republiki Sloveniji in s tem posledično tudi k zmanjšanju nezakonitih in neupravičenih posegov v zasebnost posameznika pri obdelavi osebnih podatkov, kar je poglavitni namen Zakona o varstvu osebnih podatkov in tega poročila.

---

<sup>1</sup> ZVOP-1; Uradni list RS, št. 86/2004.

## **1. KONCEPT VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI TER SPREMEMBE V LETU 2004**

Državni zbor Republike Slovenije je 15. julija 2004 sprejel novi Zakon o varstvu osebnih podatkov<sup>2</sup> (v nadaljevanju: ZVOP-1), ki je stopil v veljavo s 1. januarjem 2005. Sprejetje novega zakona je bilo potrebno predvsem zaradi vstopa Republike Slovenije v Evropsko unijo in s tem povezane dolžnosti uskladitve področja varstva osebnih podatkov z določbami Direktive 95/46/ES Evropskega Parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem gibanju takih podatkov<sup>3</sup>, pri čemer sta predlagatelj in zakonodajalec v novem zakonu že upoštevala tudi dosedanje izkušnje in pravno prakso s področja varstva osebnih podatkov.

Koncept varstva osebnih podatkov tudi po sprejetju novega zakona ostaja praktično isti kot doslej, saj je varstvo osebnih podatkov v Republiki Sloveniji ena izmed ustavno zagotovljenih človekovih pravic in temeljnih svoboščin, ki spada v okvir pravic s področja zasebnosti. V okvir teh pravic spadajo še pravica do osebnega dostojanstva in varnosti (34. člen Ustave RS), varstvo pravic zasebnosti in osebnostnih pravic (35. člen Ustave RS), nedotakljivost stanovanja (36. člen Ustave RS), varstvo tajnosti pisem in drugih občil (37. člen Ustave RS), svoboda izražanja (39. člen Ustave RS) ter svoboda vesti (41. člen Ustave RS).

Ustava Republike Slovenije<sup>4</sup> v svojem 38. členu določa:

*Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.*

*Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.*

*Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.*

Iz zgoraj citiranega 38. člena Ustave RS izhaja, da se je ustavodajalec odločil za t.i. "obdelovalni model" in ne za t.i. "model zlorabe", saj je določil predvsem pravila za urejanje dopustne obdelave osebnih podatkov na zakonski ravni in ne načelne svobode obdelave osebnih podatkov, ki je lahko le izjemoma izrecno omejena z zakonom. Takšen model preprosto pomeni, da 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. Vsaka obdelava osebnih podatkov namreč pomeni poseg v z ustavo varovano človekovo pravico do varstva osebnih podatkov, zaradi česar je takšen poseg dopusten, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo obdelovati, jasno pa mora biti razviden tudi namen obdelave osebnih podatkov ter zagotovljeno ustrezno varstvo in zavarovanje. Namen obdelave osebnih podatkov mora biti ustavno dopusten, obdelovati pa se smejo le tiste vrste osebnih podatkov, ki so primerne in nujno potrebne za uresničitev zakonsko opredeljenega namena.

Določbe 38. člena Ustave RS v bistvu predpisujejo ureditev varstva osebnih podatkov v splošnem, sistemskem zakonu, poleg tega pa dopuščajo tudi možnost urejanja varstva osebnih podatkov v področnih zakonih, ki pa morajo prav tako upoštevati določbe 38. člena Ustave RS.

---

<sup>2</sup> Uradni list RS, št. 86/2004.

<sup>3</sup> Uradni list Evropskih skupnosti št. L 281, 23.11.1995.

<sup>4</sup> UstavaRS (Uradni list RS, št. 33/91, 42/97, 66/00, 24/03 in 69/04).

Takšen koncept narekuje, da mora biti v zakonu (ne v izvršilnem predpisu!), ki ureja posamezno področje, jasno določeno, katere zbirke osebnih podatkov se bodo vzpostavile in vodile na tem področju, vrste osebnih podatkov, ki jih bodo posamezne zbirke vsebovale, način zbiranja osebnih podatkov, čas shranjevanja osebnih podatkov, morebitne omejitve pravic posameznika ter zlasti namen obdelave zbranih osebnih podatkov.

Ureditev varstva osebnih podatkov v sistemskem zakonu je potrebna zaradi enotne določitve načel, pravil in obveznosti ter zaradi zapolnitve pravnih praznin, ki bi lahko nastale v področnih zakonih, poleg tega pa je tudi nepotrebno, da bi se definicije, obveznosti in ukrepi v zvezi z zavarovanjem osebnih podatkov, katalogi zbirk osebnih podatkov, registracijo zbirk osebnih podatkov, pravicami posameznika do seznanitve s podatki, ki se nanašajo nanj, vprašanja glede nadzora ter pristojnosti nadzornega organa ipd. vedno predpisovala tudi v področnih zakonih.

Temeljni zakon, ki v Republiki Sloveniji ureja področje varstva osebnih podatkov, je od 1. januarja 2005 dalje ZVOP-1, ki kot sistemski zakon določa predvsem splošne pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov. ZVOP-1 za razliko od Zakona o varstvu osebnih podatkov, ki je veljal v letu 2004<sup>5</sup>, ni zgolj sistemski zakon, ampak je v svojem VI. delu tudi t.i. "področni zakon", ki z dokaj natančno določitvijo pravic, obveznosti, načel in ukrepov upravljavcem osebnih podatkov daje neposredno zakonsko podlago za obdelavo osebnih podatkov na področju neposrednega trženja, videonadzora, biometrije, evidentiranja vstopov in izstopov iz prostorov ter strokovnega nadzora. Gre za področja, ki do 1. januarja 2005 niso bila ustrezno zakonsko urejena.

Poleg ZVOP-1 in zakonov, ki podrobneje predpisujejo obdelavo osebnih podatkov na posameznem področju, se v Republiki Sloveniji neposredno uporabljajo tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki je bila ratificirana in objavljena leta 1994<sup>6</sup>. Namen navedene konvencije Sveta Evrope je na ozemlju vsake pogodbenice, vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotoviti spoštovanje njegovih pravic in temeljnih svoboščin in v tem okviru še posebej spoštovanje pravice do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, ki se nanašajo nanj.

Ena od bistvenih novosti ZVOP-1 je nedvomno predvidena ustanovitev povsem neodvisnega in samostojnega Državnega nadzornega organa za varstvo osebnih podatkov ter povečanje pristojnosti tega novega nadzornega organa glede na pristojnosti, ki jih je imel Inšpektorat za varstvo osebnih podatkov v letu 2004.

Po določbah ZVOP-1 bo Državni nadzorni organ za varstvo osebnih podatkov, ki naj bi pričel z delom 1. januarja 2006, zagotavljal enotno uresničevanje ukrepov na področju varstva osebnih podatkov ter s tem namenom opravljal sledeče naloge in pristojnosti:

- Opravljal inšpekcijski nadzor nad izvajanjem določb ZVOP-1, v okviru katerega naj bi se prvenstveno obravnavale prijave, pritožbe, sporočila in druge vloge, v katerih je izražen sum kršitve zakona, poleg tega pa se bo opravljal tudi preventivni inšpekcijski nadzor pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja.
- Vodil postopke o prekrških s področja varstva osebnih podatkov (hitri postopek).

---

<sup>5</sup> Zakon o varstvu osebnih podatkov (ZVOP; Uradni list RS, št. 59/99, 57/01 in 59/01 - popr., 52/02 - ZDU-1 in 73/04 - ZUP-C).

<sup>6</sup> Uradni list RS, št. 11/94 - Mednarodne pogodbe št. 3/94.

- Odločal o ugovoru posameznika glede obdelave osebnih podatkov na podlagi četrtega odstavka 9. člena in tretjega odstavka 10. člena ZVOP-1.
- Vodil upravne postopke za izdajo ugotovitvenih odločb o tem, katere tretje države imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov ter v okviru opravljanja teh nalog v Uradnem listu Republike Slovenije objavil seznam tretjih držav, za katere je ugotovil, da imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov, ali da te nimajo zagotovljene.
- Vodil upravne postopke za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo, kadar upravljavec osebnih podatkov zagotovi ustrezne ukrepe zavarovanja osebnih podatkov ter temeljnih pravic in svoboščin posameznikov in navede možnosti njihovega uresničevanja ali varstva, predvsem v določbah pogodb ali v splošnih pogojih poslovanja (70. člen ZVOP-1).
- Vodil upravne postopke 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 (npr. EMŠO ali davčna številka).
- Vodil upravne postopke za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba izvajanja biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1.
- Sodeloval 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.
- Dajal in objavljajal predhodna mnenja ministrstvu, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke.
- Dajal in objavljajal neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov.
- Dajal in objavljajal neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov.
- Pripravljajal, dajal in objavljajal neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.
- Dajal izjave za javnost o opravljenih inšpekcijskih nadzorih v posamičnih zadevah ter izvaja konference za medije v zvezi z delom organa.
- Pripravljajal in objavljajal poročila o svojem delu v preteklih letih.

Vse zgoraj navedene pristojnosti in naloge bo do pričetka dela Državnega nadzornega organa za varstvo osebnih podatkov opravljal zdajšnji Inšpektorat za varstvo osebnih podatkov. Zoper odločbe in sklepe, ki jih od 1. januarja 2005 izdaja inšpektorat in jih bo kasneje izdajal Državni nadzorni organ, ni več pritožbe, dovoljen pa je upravni spor.

V letu 2001 je Državni zbor Republike Slovenije sprejel Obligacijski zakonik<sup>7</sup>, ki v 134. členu določa, da lahko vsakdo zahteva od sodišča ali drugega pristojnega organa, da odredi prenehanje dejanja, s katerim se kršijo osebne pravice (nedotakljivost človekove osebnosti, osebne ali družinskega življenja ali kakšna druga osebna pravica), da prepreči takšno dejanje ali da odstrani njegove posledice. V povezavi s to določbo, ki ima

---

<sup>7</sup> Uradni list RS, št. 83/2001.

značaj generalne klavzule, določbe drugih členov Obligacijskega zakonika določajo pravila za povrnitev škode v takšnih primerih, npr. objavo sodbe ali popravka (178. člen), denarno odškodnino (179. člen), povrnitev škode v primeru storitve kaznivega dejanja zoper dostojanstvo osebnosti (181. člen) ter povrnitev bodoče škode (182. člen). Skoraj v celoti enake določbe so bile določene tudi v nekdanjem zveznem Zakonu o obligacijskih razmerjih SFR Jugoslavije iz leta 1978, ki je začel veljati 01.10.1978 in se je v Republiki Sloveniji uporabljal do 31.12.2001.

Zloraba osebnih podatkov je v 154. členu Kazenskega zakonika<sup>8</sup> opredeljena tudi kot kaznivo dejanje, ki se preganja po uradni dolžnosti. Določeno je, da se z denarno kaznijo ali zaporom do enega leta kaznuje, kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se podatki nanašajo ali, kdor vdre v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek. Če dejanje stori uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let.

---

<sup>8</sup> Uradni list RS, št. 95/04 - prečiščeno besedilo.

## **2. PRISTOJNOST TER ORGANIZIRANOST INŠPEKTORATA ZA VARSTVO OSEBNIH PODATKOV**

### **2.1. Pristojnosti in dolžnosti Inšpektorata za varstvo osebnih podatkov**

Inšpektorat za varstvo osebnih podatkov je v letu 2004 opravljal nadzor nad izvajanjem določb Zakona o varstvu osebnih podatkov<sup>9</sup> (v nadaljnjem besedilu: ZVOP) in drugih predpisov s področja varstva osebnih podatkov ter zagotavlja enotno uresničevanje ukrepov na tem področju.

Neposredni inšpekcijski nadzor nad izvajanjem predpisov s področja varstva osebnih podatkov je zajemal:

- nadzor nad zakonitostjo obdelave osebnih podatkov;
- nadzor nad izvajanjem postopkov in ukrepov za zavarovanje osebnih podatkov, določenih v notranjih aktih upravljavcev in uporabnikov osebnih podatkov, ter njihovo ustreznost;
- nadzor nad izvajanjem določb zakona, ki urejajo kataloge podatkov, skupni katalog osebnih podatkov in evidentiranje prenosa podatkov posameznim uporabnikom osebnih podatkov; ter
- nadzor nad izvajanjem določb zakona glede iznosa osebnih podatkov iz države in o njihovem posredovanju tujim uporabnikom.

Poleg opravljanja neposrednega inšpekcijskega nadzora je inšpektorat sodeloval z ministrstvi pri pripravi predpisov s področja osebnih podatkov ter z drugimi inšpektorati, upravnimi organi in organizacijami, zavodi, združenji in drugimi organizacijami in organi glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov.

Po določbah ZVOP je opravljal neodvisni nadzor varstva osebnih podatkov tudi Varuh človekovih pravic, ki je imel po določbah ZVOP v razmerju do Inšpektorata za varstvo osebnih podatkov, poleg ostalih, še sledeče pristojnosti:

- spremljanje dela inšpektorata in predlaganje ukrepov za izvajanje nadzorstva in za varstvo osebnih podatkov;
- lahko je predlagal inšpektoratu, da opravi nadzor in sprejme ustrezne ukrepe, vključno z začasno ali dokončno prepovedjo obdelave in uporabe osebnih podatkov, ki se obdelujejo ali uporabljajo v nasprotju z določbami zakona ali drugega predpisa;
- lahko je zahteval od inšpektorata, da poroča o ukrepih in odločitvah, ki jih je sprejel na podlagi zakona.

Inšpektorat je bil po določbah 29d. člena ZVOP dolžan v postavljenem roku obvestiti varuha o uresnitvi njegovih predlogov in priporočil ter poročati na njegovo zahtevo. Če inšpektorat predloga varuha ne bi upošteval, je bil dolžan pisno obrazložiti svojo odločitev.

Opravljanje nalog na področju varstva osebnih podatkov v razmerju do državnih organov, organov samoupravnih lokalnih skupnosti in nosilcev javnih pooblastil, ostaja tudi po sprejetju ZVOP-1 posebno področje varuha, za katerega je zadolžen eden od namestnikov varuha.

---

<sup>9</sup> Zakon o varstvu osebnih podatkov (ZVOP; Uradni list RS, št. 59/99, 57/01 in 59/01 - popr., 52/02 - ZDU-1 in 73/04 - ZUP-C); citirani zakon je veljal do 31.12.2004, za tem pa je stopil v veljavo ZVOP-1.



## **2.2. Pravice in dolžnosti inšpektorja za varstvo osebnih podatkov<sup>10</sup>**

Inšpektor za varstvo osebnih podatkov v okviru svojih pooblastil samostojno opravlja naloge inšpekcijskega nadzora. Glavni inšpektor mu lahko odvzame pooblastilo za vodenje že začetega postopka in zadevo dodeli drugemu inšpektorju ali sam prevzame vodenje postopka le v primeru, da je podan izločitveni razlog po Zakonu o splošnem upravnem postopku, ali, ko je uveden disciplinski postopek zoper inšpektorja.

Za inšpektorja za varstvo osebnih podatkov se lahko imenuje oseba, ki ima univerzitetno strokovno izobrazbo, najmanj pet let delovnih izkušenj pri delu z osebnimi podatki in strokovni izpit za inšpektorja.

Splošna načela inšpekcijskega nadzora, organizacijo inšpekcij, pravice in dolžnosti inšpektorjev, pooblastila inšpektorjev, postopek inšpekcijskega nadzora, inšpekcijske ukrepe in druga vprašanja, povezana z inšpekcijskim nadzorom, so določena v Zakonu o inšpekcijskem nadzoru<sup>11</sup>.

Specifične pravice in dolžnosti inšpektorja za varstvo osebnih podatkov so bile določene v 27e. členu ZVOP, kjer je določeno, da je pri opravljanju inšpekcijskega nadzorstva inšpektor upravičen:

- pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov ter njihov iznos iz države in posredovanje tujim uporabnikom osebnih podatkov;
- pregledovati vsebino zbirk osebnih podatkov, katalogov podatkov in skupnega kataloga osebnih podatkov;
- pregledovati dokumentacijo in akte, ki urejajo zavarovanje osebnih podatkov;
- pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;
- preverjati ukrepe in postopke za zavarovanje osebnih podatkov ter njihovo izvajanje ter;
- opravljati druge zadeve, določene z zakonom.

Če je inšpektor pri opravljanju inšpekcijskega nadzorstva ugotovil kršitev zakona ali drugega predpisa, ki ureja varstvo osebnih podatkov, je imel skladno z 28. členom ZVOP pravico takoj:

1. odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga določi;
2. odrediti prepoved obdelave osebnih podatkov subjektom, ki niso zagotovili ali ne izvajajo ukrepov in postopkov za zavarovanje osebnih podatkov ali, če nezakonito obdelujejo osebne podatke;
3. odrediti prepoved iznosa osebnih podatkov iz države in njihovega posredovanja tujim uporabnikom, če se iznašajo ali posredujejo v nasprotju z določbami zakona.

Zoper odločbo inšpektorja je bila v letu 2004 še dovoljena pritožba in sicer v osmih dneh od dneva njene vročitve. Pritožba zoper odločbo po 2. in 3. točki prvega odstavka 28. člena ZVOP ni zadržala njene izvršitve. O pritožbi je odločal minister za pravosodje v osmih dneh od vložitve. Če je inšpektor pri nadzoru ugotovil, da gre za sum storitve kaznivega dejanja ali prekrška, je

---

<sup>10</sup> Navedene so pravice in dolžnosti, ki jih je imel inšpektor za varstvo osebnih podatkov v letu 2004. Specifične pravice in dolžnosti inšpektorja so bile določene v 27č., 27d., 27e., 28., 28a., 28b. in 28c. členu ZVOP. V novem ZVOP-1, ki valja od 1. januarja 2005, so specifične pravice in dolžnosti inšpektorja (bodočega državnega nadzornika za varstvo osebnih podatkov) določene v 43., 44., 50., 51., 52., 53., 54., 55., 56. in 58. členu ZVOP-1.

<sup>11</sup> Uradni list RS, št. 56/2002.

podal kazensko ovadbo oziroma predlog za uvedbo postopka o prekršku.

V primeru, ko je inšpektor pri opravljanju inšpekcijskega nadzorstva ugotovil nezakonnosti v zvezi z varstvom osebnih podatkov, je o svoji ugotovitvi seznanil tudi prizadete, če je šlo za ugotovitve, ki imajo splošen pomen, pa je lahko seznanil tudi medije.

Da ne bi prišlo do morebitnih kršitev informacijske zasebnosti posameznikov v zvezi z izvajanjem inšpekcijskega nadzorstva, je bilo v 28c. členu ZVOP določeno, da je inšpektor osebne podatke, s katerimi se seznanil pri izvajanju inšpekcijskega nadzorstva, dolžan varovati kot uradno tajnost, tudi po prenehanju opravljanja službe inšpektorja. Ta dolžnost je veljala tudi za vse zaposlene delavce v inšpektoratu.

### **2.3. Organizacija in kadrovska zasedenost Inšpektorata za varstvo osebnih podatkov ter problematika v zvezi s tem**

Inšpektorat za varstvo osebnih podatkov deluje kot samostojen organ v sestavi Ministrstva za pravosodje. Takšno organiziranost narekujejo določbi 27. člena ZVOP ter 8. člena Zakona o inšpekcijskem nadzoru, poleg tega pa takšno organizacijo predpisuje tudi 13. člen Uredbe o organih v sestavi ministrstev<sup>12</sup>. Opisana organiziranost nadzornega organa se bo spremenila s 1. januarjem 2006, ko bo inšpekcijski nadzor nad izvajanjem določb ZVOP-1 in drugih predpisov s področja varstva osebnih podatkov pričel opravljati Državni nadzorni organ za varstvo osebnih podatkov in v tem organu zaposleni državni nadzorniki za varstvo osebnih podatkov.

V letu 2004 je Inšpektorat za varstvo osebnih podatkov porabil skupaj 33.677.000 SIT proračunskega denarja. Od navedenega zneska se je porabilo:

- 29.500.000 SIT za plače, druge izdatke zaposlenim ter prispevke za socialno varnost;
- 3.679.000 SIT za blago, potne stroške in storitve;
- 488.000 SIT za investicije in investicijsko vzdrževanje.

Inšpektorat za varstvo osebnih podatkov nima notranjih organizacijskih enot ter opravlja predvsem naloge inšpekcijskega nadzora ter druge strokovne naloge, ki mu jih v zvezi z varstvom osebnih podatkov nalaga zakon.

Naloge strokovne pomoči na področju upravljanja s kadrovskimi, finančnimi, informacijskimi in drugimi viri je za inšpektorat opravljalo Ministrstvo za pravosodje.

Notranjo organizacijo in sistematizacijo delovnih mest inšpektorata določa *Pravilnik o notranji organizaciji in sistematizaciji delovnih mest Inšpektorata za varstvo osebnih podatkov*, ki velja od 13.11.2001. V navedenem aktu so od februarja 2004 sistematizirana le 3 delovna mesta in sicer: glavni inšpektor, inšpektor svetnik in tajnica, kar pomeni tudi dejansko število zaposlenih na inšpektoratu v letu 2004. Navedeno število zaposlenih je po našem mnenju občutno premajhno za uspešno opravljanje vseh nalog in pristojnosti, ki jih zakon nalaga inšpektoratu.

Premajhno število zaposlenih ter povečanje obsega prejetih prijav in zaprosil za mnenja in tolmačenja ter zaradi vstopa Republike Slovenije v Evropsko unijo povečanje obsega sodelovanja Inšpektorata za varstvo osebnih podatkov na mednarodnem področju, je botrovalo k zmanjšanju opravljanja tako imenovanih preventivnih inšpekcijskih pregledov.

---

<sup>12</sup> Uradni list RS, št. 58/03.

Ker zaenkrat nič ne kaže na to, da se bo število drugih nalog, ki jih inšpektorat opravlja poleg nalog neposrednega inšpekcijskega nadzora, v bližnji prihodnosti zmanjšalo (ZVOP-1 s 1. januarjem 2005 obseg teh nalog in pristojnosti še bistveno povečuje), bi bilo število tako imenovanih preventivnih pregledov možno povečati le na ta način, da se omeji opravljanje drugih nalog, kar pa se nam ne zdi smiselno, ali pa da se čimprej poveča število inšpektorjev za varstvo osebnih podatkov.

V zvezi z izvajanjem nalog Inšpektorata za varstvo osebnih podatkov je potrebno upoštevati, da se osebni podatki obdelujejo praktično na vseh področjih javnega in zasebnega sektorja. To pa pomeni, da mora Inšpektorat za varstvo osebnih podatkov opravljati inšpekcijski nadzor pri upravljavcih osebnih podatkov na različnih specifičnih področjih, kot so npr.: državna uprava, pravosodje, lokalna samouprava, gospodarske javne službe, zdravstvo, vzgoja in izobraževanje, zavarovalništvo, bančništvo, zasebno varovanje, detektivska dejavnost, delovne evidence, ipd. Pri tem je seveda jasno, da samo dva inšpektorja, ki sta sedaj zaposlena na Inšpektoratu za varstvo osebnih podatkov, ne moreta učinkovito nadzirati upravljavcev osebnih podatkov vseh prej navedenih področjih.

### **3. AKTIVNOSTI INŠPEKTORATA ZA VARSTVO OSEBNIH PODATKOV V LETU 2004**

#### **3.1. Inšpekcijski nadzor nad izvajanjem določb ZVOP**

V letu 2004 je Inšpektorat za varstvo osebnih podatkov prejel skupaj 78 prijav, pritožb, sporočil in drugih vlog, ki so bile vložene zaradi suma kršitev določb ZVOP. Trend povečevanja števila prijav, pritožb in drugih vlog v zvezi s sumom kršitve določb ZVOP se je tako nadaljeval tudi v letu 2004.

Razloge za precejšnje povečanje števila prijav glede na pretekla leta pripisujemo predvsem večji prepoznavnosti Inšpektorata za varstvo osebnih podatkov ter večji osveščenosti posameznikov glede dolžnosti varovanja njihovih osebnih podatkov s strani upravljavcev osebnih podatkov.

Za primerjavo navajamo število prijav, pritožb, sporočil in drugih vlog, ki so bile zaradi suma kršitev določb ZVOP vložene od leta 1996 naprej:

- leta 1996: 25
- leta 1997: 27
- leta 1998: 33
- leta 1999: 26
- leta 2000: 35
- leta 2001: 43
- leta 2002: 52
- leta 2003: 60
- leta 2004: 78

Prijave oziroma pritožbe, ki so bile v letu 2004 vložene zaradi suma kršitev določb ZVOP, so bile vložene iz sledečih razlogov:

- 7 zaradi suma posredovanja osebnih podatkov nepooblaščenim uporabnikom;
- 6 zaradi neustreznega zavarovanja osebnih podatkov;
- 6 zaradi uporabe osebnih podatkov za namene neposrednega trženja;
- 6 zaradi suma prekomernega in nezakonitega zbiranja osebnih podatkov;
- 5 zaradi izobešanja seznamov dolžnikov in seznamov stanovalcev na oglasne deske v večstanovanjskih stavbah;
- 5 zaradi suma nezakonitega posredovanja osebnih podatkov javnosti in objave osebnih podatkov v sredstvih javnega obveščanja;
- 4 zaradi suma kršitve pravic posameznika v zvezi s podatki, ki se nanašajo nanj (18. in 19. člen ZVOP);
- 4 zaradi izvajanja videonadzora;
- 3 zaradi zbiranja in uporabe osebnih podatkov za namene odločanja v upravnih postopkih;
- 3 zaradi suma nezakonitega slikovnega snemanja;
- 3 zaradi suma nezakonite obdelave osebnih podatkov za namene izvajanja javnih služb;
- 2 zaradi suma nezakonitega navajanja podatkov o zdravstvenem stanju v odločbah ZZS;
- 2 zaradi suma nezakonitega zbiranja osebnih podatkov za namene sodnih postopkov;
- 2 zaradi suma nezakonite obdelave osebnih podatkov ustanoviteljev, zastopnikov, vodstva in članov nadzornega sveta pravnih subjektov;
- 2 zaradi suma posredovanja baze podatkov ZZS zasebni zavarovalnici;

- 2 zaradi suma nezakonite obdelave osebnih podatkov s strani policije.

Po 1 prijava oziroma pritožba je bila vložena iz sledečih razlogov:

- sum nezakonite uporabe osebnih podatkov za namene izvedbe ankete;
- sum kršitve zakona zaradi priložitve pobude skupine občanov k računom za KATV;
- sum kršitve zakona z izobešanjem sodbe na oglasno desko v podjetju – toženi stranki;
- sum kršitve zakona zaradi kontrole bolniškega staleža;
- sum kršitve zakona zaradi združitve več upravnih zadev v en postopek, zaradi česar naj bi se stranke s prejemom odločbe neupravičeno seznanile z osebnimi podatki drugih strank;
- sum kršitve zakona zaradi kopiranja dokumentacije s strani banke za namene izvedbe transakcije;
- sum nezakonitega pridobivanja osebnih podatkov za namene vodenja postopkov o prekrških;
- sum nezakonitega zbiranja osebnih podatkov o pacientu s strani osebnega zdravnika;
- sum nezakonitega posredovanja zdravstvene kartoteke delodajalcu;
- sum kršitve zakona z objavo osebnega imena in kraja bivališča osebe, ki je bila izžrebana na javnem žrebanju;
- sum nezakonite uporabe osebnih podatkov iz evidence prekrškov;
- sum nezakonitega posredovanja osebnih podatkov domnevnega dolžnika osebam v kraju njegovega bivanja;
- sum kršitve zakona zaradi zasledovanja lastnika vozila;
- zaradi neizdelanih katalogov zbirk osebnih podatkov;
- zaradi grožnje zaposlenim na eni od osnovnih šol;
- zaradi objave osebnih podatkov udeležencev nagradne igre na spletnih straneh organizatorja nagradne igre.

Poleg obravnavanja navedenih prijav in pritožb je inšpektorat v letu 2004 obravnaval še 22 zadev v okviru katerih se je opravljal preventivni inšpekcijski nadzor nad izvajanjem določb ZVOP. Preventivni nadzor se je opravljal predvsem pri upravljavcih osebnih podatkov na področju državne uprave, pravosodja, zdravstvenega varstva, vzgoje in izobraževanja, lokalne samouprave ter delovnih evidenc.

Zaradi ugotovljenih večjih nepravilnosti oziroma kršitev ZVOP je bilo v letu 2004 izdanih 6 upravnih odločb, podanih 13 predlogov za uvedbo postopka o prekršku ter 2 kazenski ovadbi.

Zaradi ugotovljenih manjših nepravilnosti je bilo v letu 2004 na podlagi 33. člena Zakona o inšpekcijskem nadzoru izrečenih tudi 32 opozoril za odpravo nepravilnosti na zapisniku. Ustna opozorila so bila izrečena zaradi ekonomičnosti postopka, učinkovitosti ukrepa ter iz razloga, ker zadeve pri sodniku za prekrške v veliki večini primerov zastarajo.

Kot manjše nepravilnosti, zaradi katerih je inšpektor namesto izdaje upravne odločbe in podaje predloga za uvedbo postopka o prekršku izrekel zgolj opozorilo na zapisniku, štejemo tiste nepravilnosti, zaradi katerih ni bilo neposrednega posega v pravice posameznikov oziroma nepravilnosti niso imele za posledico kršitve informacijske zasebnosti posameznika. Takšne manjše nepravilnosti so predvsem pomanjkljivi katalogi zbirk podatkov, pomanjkljivi oziroma ne dovolj dodelani notranji akti za zavarovanje osebnih podatkov, pomanjkljivo določeni pogoji in ukrepi za zagotovitev varstva in zavarovanja osebnih podatkov v pogodbah s pogodbenimi obdelovalci, manjše pomanjkljivosti v zvezi z izvajanjem postopkov

in ukrepov za zavarovanje osebnih podatkov ter pomanjkljive in nejasne pisne privolitve posameznikov.

Pri sodnikih za prekrške so bile v letu 2004 v zvezi s predlogi, ki jih je podal Inšpektorat za varstvo osebnih podatkov, izdane 3 odločbe. V 2 primerih je bila kršiteljem izrečena denarna kazen, v 1 primeru pa je sodnik za prekrške postopek ustavil, ker naj dejanje ne bi bilo prekršek.

V okviru obravnave prijav in pritožb v zvezi s sumom kršitev določb ZVOP je inšpektorat v 8 obravnavanih primerih ugotovil, da zavezanec s svojim ravnanjem ni kršil določb ZVOP ter v zvezi s tem na podlagi 28. člena Zakona o inšpekcijskem nadzoru izdal sklep o ustavitvi postopka. Poleg tega je bilo v primeru 17 prijav in pritožb že iz samih prijav razvidno, da opisano dejanje ne pomeni kršitve določb ZVOP, zaradi česar je inšpektor prijaviteljem v teh primerih namesto uvedbe postopka zgolj pisno pojasnil razloge, zaradi katerih opisano dejanje ne pomeni kršitve določb ZVOP in zaradi katerih bi bila uvedba postopka inšpekcijskega nadzora nesmiselna. Zoper takšno pojasnilo je vložil ugovor le 1 prijavitelj, nakar je inšpektor po prejemu ugovora izvedel postopek inšpekcijskega nadzorstva ter na podlagi ugotovitev v tem postopku izdal sklep o ustavitvi postopka, saj je izvedeni postopek potrdil, da v zadevi ni šlo za kršitev določb ZVOP. Prijavitelj zoper izdani sklep ni vložil pritožbe.

Iz zgoraj navedenih podatkov izhaja, da je inšpektorat pri reševanju prijav in pritožb ter pri opravljanju preventivnega inšpekcijskega nadzora v letu 2004 večje kršitve določb ZVOP ugotovil le v 20% zadev (podana je bila kazenska ovadba ali predlog za uvedbo postopka o prekršku), v 47% zadev so bile ugotovljene le manjše nepravilnosti (izrečeno je bilo ustno opozorilo), v 35% zadev pa kršitve sploh niso bile ugotovljene.

V letu 2004 so bile vložene 3 pritožbe zoper odločbe, ki jih je izdal inšpektor za varstvo osebnih podatkov, in sicer:

1. pritožba je bila vložena zoper odločbo, s katero je inšpektor Banki Slovenije naložil, da prek svoje spletne strani onemogoči dostop do podatkov o transakcijskih računih o tistih fizičnih osebah, ki niso zasebniki, in sicer vse do takrat, dokler banka za te osebe ne bo zagotovila, da bo mogoče za vsako takšno posredovanje podatkov pozneje ugotoviti, kateri osebi so se v določenem obdobju posredovali podatki iz registra transakcijskih računov o tistih fizičnih osebah, ki niso zasebniki. Ministrica za pravosodje je kot organ druge stopnje zaradi napačne uporabe materialnega predpisa odpravila odločbo inšpektorja in hkrati sama odločila o stvari. Odločila je tako, da je Banki Slovenije odredila, da takoj po vročitvi njene odločbe, onemogoči dostop prek svoje spletne strani do podatkov o transakcijskih računih tistih fizičnih oseb, ki niso zasebniki.
2. pritožba je bila vložena zoper odločbo, s katero je inšpektor enemu od državnih organov naložil, da v 2 dneh po vročitvi odločbe zagotovi, da se bodo zavezancem pošiljale odločbe le še v neprosojnih ovojnicah, pri katerih ob normalni svetlobi oziroma pri osvetlitvi ovojnic z običajno lučjo ne bo vidna vsebina ovojnice oziroma ne bodo vidni osebni podatki, ki jih odločba vsebuje. Ministrica za pravosodje je kot organ druge stopnje pritožbo organa zoper inšpektorjevo odločbo v celoti zavrnila.
3. pritožba je bila vložena zoper odločbo, s katero je inšpektor eni od slovenskih občin naložil, da v roku 10 dni po vročitvi odločbe v Evidenci prekrškov zagotovi, da se po preteku določenih rokov onemogoči vsakršna nadaljnja obdelava sledečih osebnih podatkov, ki se nanašajo na kršitelje: št. registrske tablice, priimek in ime, datum rojstva, EMŠO ter naslov stalnega ali začasnega bivališča. Zavezanec je v svoji pritožbi navedel,

da se strinja glede odprave nepravilnosti v zvezi z vodenjem Evidence prekrškov, da pa je rok za izvedbo zahtev, navedenih v izreku odločbe prekratek. Pritožbi je inšpektor ugodil ter na podlagi prvega odstavka 242. člena Zakona o splošnem upravnem postopku z novo odločbo nadomestil izpodbijano odločbo. Nova odločba se je od prvotne odločbe razlikovala le v tem, da se je rok, v katerem mora zavezanec onemogočiti nadaljnjo obdelavo določenih osebnih podatkov v Evidenci prekrškov, podaljšal z 10 na 30 dni.

Poleg pritožb zoper odločbe, s katerimi je inšpektor odredil prepoved obdelave osebnih podatkov ali pa zavezancu naložil odpravo ugotovljenih nepravilnosti, je bila v letu 2004 vložena tudi 1 pritožba zoper sklep, s katerimi je inšpektor iz razloga, ker v postopku niso bile ugotovljene kršitve določb ZVOP, ustavil postopek inšpekcijskega nadzora. Pritožba je bila vložena prepozno, zaradi česar jo je organ prve stopnje s sklepom zavrgel.

Od skupaj natanko 100 zadev inšpekcijskega nadzora, ki jih je Inšpektorat za varstvo osebnih podatkov v letu 2004 uvedel bodisi zaradi prijav oziroma pritožb posameznikov, bodisi zaradi opravljanja preventivnega nadzora, je do 1. januarja 2005 ostalo nerešenih skupaj 28 zadev. Gre predvsem za tiste zadeve, ki so bile uvedene v zadnjem četrtletju leta 2004.

### **3.2. Ostale aktivnosti inšpektorata na domačem področju**

Na domačem področju je bilo v obravnavanem obdobju evidentiranih tudi 43 zadev, v okviru katerih so se podajala pisna mnenja in pojasnila v zvezi s konkretnimi vprašanji, ki so jih na inšpektorat v zvezi z varstvom osebnih podatkov na posameznih področjih naslavljale razne pravne in fizične osebe.

Zaprosila za mnenja in tolmačenja se nanašajo na različna področja, pri čemer še vedno prevladujejo zaprosila za mnenja in tolmačenja s področja notranjih zadev, lokalne samouprave, zdravstvenega varstva in zavarovanja, pravosodja, upravljanja večstanovanjskih stavb ter delovnih razmerij.

Podajanje pisnih mnenj in tolmačenj glede obdelave osebnih podatkov na posameznih področjih je vsekakor zelo pomemben del preventivnega delovanja Inšpektorata za varstvo osebnih podatkov, ki po našem mnenju precej prispeva k izboljšanju varstva osebnih podatkov v Republiki Sloveniji. Vendar pa občutno povečevanje števila zaprosil za mnenja in tolmačenja v zvezi z varstvom osebnih podatkov obema inšpektorjema jemlje zelo veliko časa, zaradi česar je bilo v letu 2004 obravnavanih manj zadev neposrednega preventivnega inšpekcijskega nadzora, kot bi jih po našem mnenju morale biti.

Poleg podaje pisnih mnenj in tolmačenj, je inšpektorat v okviru preventivnega delovanja opravljal tudi sledeče aktivnosti:

- vsakodnevno prek telefona in elektronske pošte posredoval informacije ter kratka mnenja, stališča in tolmačenja v zvezi z vprašanji, ki se nanašajo na varstvo osebnih podatkov;
- obveščal javnost o stanju na področju varstva osebnih podatkov ter o delu Inšpektorata za varstvo osebnih podatkov;
- sodeloval na seminarjih, konferencah, posvetih in sestankih, kjer se je obravnavala tudi problematika varstva osebnih podatkov;
- opozarjal in nudil pomoč upravljavcem osebnih podatkov z različnih področij pri ureditvi katalogov podatkov ter pri pripravi ustreznih pisnih privolitev posameznikov za obdelavo

- osebnih podatkov;
- nudil pomoč pri določanju organizacijskih in ustreznih logično tehničnih postopkov in ukrepov za zavarovanje osebnih podatkov ter pri pripravi ustreznih notranjih aktov.

Pri vsakodnevnem posredovanju mnenj upravljavcem osebnih podatkov ter posameznikom še vedno ugotavljamo, da upravljavci osebnih podatkov ter posamezniki določb ZVOP bodisi ne poznajo dovolj dobro, ali pa posameznih določb oziroma koncepta varstva osebnih podatkov v Republiki Sloveniji preprosto ne razumejo. Ob tem je potrebno tudi opozoriti, da se v praksi žal še vedno dogaja, da posamezni predstavniki upravljavcev osebnih podatkov, ki se s svojimi vprašanji obračajo na inšpektorat, ZVOP pred tem sploh ne preberejo.

Zaradi nerazumevanja posameznih določb ZVOP je inšpektorat v preteklih poročilih o svojem delu navajal podrobnejša pojasnila v zvezi s tistimi določbami ZVOP, zaradi katerih so se upravljavci osebnih podatkov ter posamezniki najpogosteje obračali na inšpektorat ter prosili za mnenja oziroma tolmačenja glede uporabe določb ZVOP na posameznih področjih. Kljub temu se je trend naraščanja števila zaprosil za mnenja in tolmačenja v zvezi z varstvom osebnih podatkov nadaljeval tudi v letu 2004. Število zaprosil za mnenja in tolmačenja se je še posebej povečalo po sprejetju ZVOP-1, kar pa se zdi povsem razumljivo, saj so v novem zakonu nekatera področja (neposredno trženje, videonadzor, biometrija, evidence vstopov in izstopov iz prostorov, povezovanje zbirk osebnih podatkov, strokovni nadzor) urejena povsem na novo.

Podobno kot prejšnja leta je inšpektorat tudi v letu 2004 aktivno sodeloval z ministrstvi in drugimi organi ter organizacijami pri pripravi zakonov in drugih predpisov, ki na posameznih področjih predpisujejo obdelavo osebnih podatkov. V zvezi s tem velja zlasti izpostaviti sodelovanje inšpektorata pri pripravi predloga ZVOP-1 ter pri pripravi predloga sprememb in dopolnitev 45. člena Zakona o medijih. Inšpektorat za varstvo osebnih podatkov je v zvezi s 45. členom Zakona o medijih, ki ureja posredovanje informacij urednikom, novinarjem in drugim avtorjem programskih prispevkov predlagal, da se 45. člen dopolni tako, da se v njem natančno določi, katere vrste osebnih podatkov se v določenih primerih lahko posredujejo medijem, s čimer bi mediji pridobili neposredno zakonsko podlago za pridobivanje določenih osebnih podatkov. Pripravljen predlog kasneje ni bil sprejet, zaradi česar se lahko medijem oziroma javnosti zaradi strogih določb Zakona o varstvu osebnih podatkov posredujejo osebni podatki le v primeru, če je v nekem področnem zakonu izrecno določeno, da so določeni osebni podatki javni, ali pa, če se z njihovo objavo lahko prepreči hujše kaznivo dejanje ali neposredna nevarnost za življenje ljudi in njihovo premoženje.

### **3.3. Aktivnosti inšpektorata na mednarodnem področju**

Na mednarodnem področju je Inšpektorat za varstvo osebnih podatkov aktivno sodeloval pri pripravi skupnih osnov in posameznih dokumentov varstva osebnih podatkov v Evropski uniji, sodeloval pri pripravi dokumentov v okviru Direktorata za pravico, svobodo in varnost ter sodeloval na sestankih skupnih nadzornih organov za Europol, Eurojust, Schengen in Carino.

V obravnavanem obdobju je Republika Slovenija postala polnopravna članica Evropske unije, zaradi česar se je sodelovanje inšpektorata s pristojnimi organi Evropske unije, drugimi mednarodnimi organizacijami ter s tujimi nadzornimi organi precej povečalo. Aktivno smo sodelovali predvsem v sledečih mednarodnih organih oziroma skupinah:

1. CJ-PD, Projektna skupina za varstvo osebnih podatkov v Svetu Evrope;



2. T-PD, Posvetovalni odbor Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v Svetu Evrope;
3. T-PD-GR, Redakcijska skupina posvetovalnega obora Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v Svetu Evrope;
4. Delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov, ki je ustanovljena na podlagi 29. člena Direktive 95/46/ES;
5. Skupni nadzorni organ Evropske unije za EURODAC;
6. Skupni nadzorni organ Europol;
7. Skupni nadzorni urad za Schengen;
8. Skupni nadzorni urad za Carino.

V okviru sodelovanja inšpektorata na mednarodnem področju, smo se v letu 2004 udeležili sledečih sestankov:

Dne 28. januarja 2004 smo v Bruslju na sestanku Delovne skupine za zaščito posameznikov pri obdelavi osebnih podatkov razpravljali o tem, kako skladno z dokumenti EU ter Direktivo 95/46/ES urediti obdelavo (posredovanje) osebnih podatkov potnikov, ki potujejo v ZDA.

Problematika zahteva tehtanje med zasebnostjo in interesi zavarovanja varnosti, kar naša zakonodaja sicer omogoča, vprašanje je le koliko to posega v "informacijsko zasebnost" posameznika. Naša ocena je, da so zahteve uresničljive skladno z našim zakonom o varstvu osebnih podatkov.

Dne 29. januarja 2004 smo se v Bruslju udeležili sestanka Delovne skupine za zaščito posameznikov pri obdelavi osebnih podatkov, ki je obravnavala problematiko glede zaščite (varstvo in zavarovanje) posameznikov pri obdelavi osebnih podatkov - razkrivanju osebnih podatkov tretjim državam, izven Evropske skupnosti.

Dne 16. februarja 2004 smo v Bruslju na sestanku Odbora iz 31. člena Direktive 95/46/ES, ki Komisiji pomaga pri delu, obravnavali problematiko v zvezi z zavarovanjem posameznih osebnih podatkov potnikov, ki potujejo v ZDA ter problematiko v zvezi z razkrivanjem teh podatkov Uradu za carinsko in mejno zaščito Združenih držav Amerike CBP (Customs and Border protection) za potrebe obdelave PNR (passenger name record).

Dne 5. maja 2004 smo v Bruslju na sestanku Odbora iz 31. člena Direktive 95/46/ES obravnavali odločbo Komisije o ustreznem varstvu osebnih podatkov, vsebovanih v zapisu podatkov o letalskih potnikih PNR (passenger name record) za posredovanje Uradu za carinsko in mejno zaščito Združenih držav Amerike (CBP - Customs and Border protection).

Obravnavali smo tudi dokument glede zaščite (varstva in zavarovanja) osebnih podatkov PNR za potrebe letalskih prevozov v Avstralijo ter informacijo in mnenja glede standardov za obdelavo (posredovanje osebnih podatkov tretjim državam) določenih osebnih podatkov v okviru ICC (International Chamber of Commerce) in drugih poslovnih asociacijah. Na sestanku smo pregledali omenjene dokumente in se do odločbe Komisije pozitivno opredelili.

Dne 21. in 22. junija 2004 smo v Bruslju na sestanku Delovne skupine za zaščito posameznikov pri obdelavi osebnih podatkov obravnavali:

- dokument v zvezi z Direktivo 2002/58 ES, glede zaščite osebnih podatkov v telekomunikacijskem sektorju;
- delovni program;
- nove dosežke na področju varstva osebnih podatkov španskega nadzornika;
- rešitve varstva osebnih podatkov glede PNR (osebni podatki potnika) v ZDA, Avstraliji in Kanadi;
- poročilo o uporabi podatkov v internetu na temelju Direktive 2002/58 ES;
- uporabo biometričnih elementov za Evropski informacijski sistem (vize) VIS;
- uporabo prometnih podatkov;
- predstavitev novega sistema elektronske pošte Google;
- kako učinkoviteje implementirati določbe direktive 95/46/ES;
- uporabo pravil varstva osebnih podatkov pri obdelavi podatkov, (Daimler Crhrysler, General Electric company, Philips) in implementacijo pravil varstva;
- informacijo o iznosu podatkov v države, ki ne zagotavljajo varstva osebnih podatkov v skladu z Direktivo 95/46/ES (26 . člen Direktive).

Dne 14., 15., in 16. septembra 2004 smo sodelovali na 26. mednarodni konferenci o zasebnosti in varstvu osebnih podatkov v Wroclawu na Poljskem. Obravnavali smo probleme, ki so povezani predvsem s hitrim razvojem tehnike in tehnologije, ki v veliki meri vplivajo na zaščito, varstvo in zavarovanje osebnih podatkov.

Udeležili smo se treh paralelnih razprav, kjer smo obravnavali vpliv medijev na varstvo osebnih podatkov, varstvo in zavarovanje osebnih podatkov v Internetu, kakor tudi vpliv biometrije na vsebino obdelave osebnih podatkov.

Na zaprtem delu konference smo obravnavali mednarodne probleme zaščite osebnih podatkov in probleme evropskih nadzornikov.

Dne 14. in 15. oktobra 2004 smo sodelovali na mednarodni konferenci o varstvu osebnih podatkov, ki jo je organiziral Svet Evrope in Češki Urad za varstvo osebnih podatkov. Obravnavali smo probleme, ki so posledica hitrega razvoja tehnike in tehnologije, ki v veliki meri vplivajo na zaščito, varstvo in zavarovanje osebnih podatkov. Glavni poudarek je bil na posamezniku, torej na subjektu, na katerega se osebni podatki nanašajo.

Razpravljali smo o problematiki v zvezi s privolitvijo posameznika glede posameznih obdelav osebnih podatkov; o zavarovanju podatkov glede obdelav za druge namene, to je za namene, ki niso zajeti v privolitvi; o tem, kako upravljavec osebnih podatkov zagotavlja zaščito (varstvo in zavarovanje) obdelave osebnih podatkov za katere ima določeno soglasje ter, ali to tudi preseže. Konferenca je želela dati odgovor na to, kako v širitvi svetovnih povezav zaščititi, varovati in zavarovati obdelavo osebnih podatkov. Enoličnega odgovora ni bilo.

Dne 22. novembra 2004 smo v Bruslju na povabilo GD Justice and home Affairs sodelovali na sestanku, kjer smo obravnavali, kako urediti obdelavo (posredovanje) osebnih podatkov skladno z dokumenti EU, Direktivo 95/64/ES in posredovanje podatkov drugim uporabnikom

ter policiji za odpravljanje kriminalnih dejanj.

Odločitev zahteva tehtanje med zasebnostjo in interesi zavarovanja varnosti, kar naša zakonodaja sicer omogoča, vprašanje je le koliko to posega v "zasebnost" posameznika. Naša ocena je, da so zahteve uresničljive skladno z našim veljavnim ZVOP-1.

Udeleženci razprav so bili mnenja, da je boj proti kriminalu in terorizmu pomemben, potrebne pa so pravne podlage za pridobivanje podatkov, za hitro ukrepanje in dokaj lahek dostop do določenih osebnih podatkov.

Dne 23. novembra 2004 smo v Bruslju sodelovali na sestanku nadzornikov za Europol, Eurojust, Schengen in Carino, kjer smo kot vsebinsko točko obravnavali sodelovanje s Svetom in Evropskim parlamentom glede izmenjave podatkov in informacij za boj proti terorizmu in ostalemu kriminalu.

Dne 20. decembra 2004 smo v Bruslju sodelovali na sestanku Skupnega nadzornega telesa Europol (JSB Europol) in Skupnega nadzornega organa za carino (JSA Customs).

Na sestanku Skupnega nadzornega telesa Europol smo obravnavali 24.(4) člen Konvencije Europol; napredek pri pripravi novega Europol Index Sistema; sredstva za delo Skupnega nadzornega organa - pravila; sredstva za delo Skupnega nadzornega organa za leto 2006; nadzor Europol v marcu 2005; spletno stran Skupnega nadzornega telesa; pravila za posredovanje in objavljanje dokumentov; izvolitev podpredsednika Skupnega nadzornega telesa.

Na sestanku Skupnega nadzornega organa za področje Carine smo obravnavali vzpostavitev CIS carinskega informacijskega sistema; imeli sestanek z g. Tjalkensom (CCWG), Staedegem (CCWG), in go. Evo Mario Meyer, predstavniko OLAF; ter poročilo o nadzoru izvrševanja sistema CIS;

Dne 21. decembra 2004 smo v Bruslju na sestanku Skupnega nadzornega telesa Europol - odbora za pritožbe (JSB AC), Skupnega nadzornega organa za Schengen (JSA SCH) in sestanka skupnega nadzornega organa za Europol, Eurojust, Schengen in Carino (JSA EP, EJ, SCH in CU) obravnavali poročilo o pritožbi, ki je bila vložena na Pritožbeno komisijo Europol.

Na sestanku Skupnega nadzornega organa za Schengen smo obravnavali napredek (ustno poročilo) SIS II (Schengenski informacijski sistem); člen 96 glede nadzora ter implementacijo SIS (Schengenski informacijski sistem).

Na sestanku skupnega nadzornega organa Europol, Eurojust, Schengen in Carine (JSA EP, EJ, SCH in CU) smo se seznanili z izhodišči Komisarja g. Franca Frattinia, Komisarja odgovornega za Pravico, svobodo in varnost ter obravnavali osnutek dokumenta glede določenih sprememb zakonodaje glede varstva osebnih podatkov.

#### **4. PREGLED IN OCENA STANJA VARSTVA OSEBNIH PODATKOV NA PODROČJIH, NA KATRERIH SE JE V LETU 2004 OPRAVLJAL INŠPEKCIJSKI NADZOR**

##### **4.1. Državna uprava**

V obravnavanem obdobju je inšpektorat prejel 3 pritožbe zoper organe državne uprave. Vse tri pritožbe so bile vložene zaradi suma nezakonitega zbiranja in uporabe osebnih podatkov za namene vodenja upravnih postopkov ter so se kasneje v postopku izkazale za neutemeljene.

Kljub temu, da pri obravnavi prijav posameznikov kršitve določb ZVOP niso bile ugotovljene, pa je na tem mestu potrebno opozoriti, da bodo morala ministrstva in drugi državni organi v bodoče veliko več pozornosti posvetiti zlasti ureditvi katalogov zbirk osebnih podatkov ter posredovanju podatkov iz teh katalogov državnemu nadzornemu organu za varstvo osebnih podatkov, ki vodi Register zbirk osebnih podatkov (bivši Skupni katalog osebnih podatkov). Pregled Registra zbirk osebnih podatkov, ki ga zaenkrat vodi še Ministrstvo za pravosodje, namreč kaže, da so podatki, objavljeni v registru zastareli in ne odražajo dejanskega stanja.

V preteklosti smo že opozarjali na problematiko v zvezi z evidentiranjem obiskovalcev, ki vstopajo v posamezna ministrstva ter videonadzorom, povezanim z varovanjem objektov. Državni organi do 1. januarja 2005, ko je stopil v veljavo ZVOP-1, za vodenje evidence vstopov in izstopov v zgradbe ter za opravljanje videonadzora sploh niso imeli ustrezne zakonske podlage. Pravno praznino v zvezi s tem je ZVOP-1 sicer odpravil, vendar pa bodo morala ministrstva in drugi državni organi vodenje evidence vstopov in izstopov v njihove prostore ter izvajanje videonadzora uskladiti z določbami ZVOP-1, poleg tega pa bodo morali za takšne evidence zagotoviti kataloge zbirk osebnih podatkov, podatke iz katalogov bodo morali posredovati nadzornemu organu (do 1. januarja 2006 bo to Ministrstvo za pravosodje), zagotoviti bo potrebno ustrezno zavarovanje takšnih podatkov ter določiti osebe, ki so odgovorne za posamezne zbirke in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene podatke. V primeru, da bodo z videonadzornim sistemom in evidenco vstopov in izstopov opravljale druge osebe (npr. družbe za zasebno varovanje ali policija), bodo morali državni organi s temi osebami skleniti tudi pogodbe, ki jih predpisuje 11. člen ZVOP-1.

Nekatera ministrstva in njihovi organi v sestavi ter drugi državni v svojih notranjih aktih pogosto še vedno nimajo predpisanih organizacijskih in ustreznih logično tehničnih postopkov in ukrepov za zavarovanje osebnih podatkov, oziroma so takšni akti pogosto zastareli, poleg tega pa zaposleni s takšnimi akti mnogokrat sploh niso seznanjeni.

Kar zadeva zavarovanje osebnih podatkov tudi ugotavljamo, da ministrstva in drugi državni organi, ki posamezna opravila v zvezi z obdelavo osebnih podatkov zaupajo pogodbenim obdelovalcem (7. člen ZVOP in 11. člen ZVOP-1), v takšnih pogodbah pogosto pomanjkljivo predpišejo postopke in ukrepov za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

Na področju upravnih enot se kaže potreba po ustanovitvi posebne delovne skupina, ki bi v sodelovanju s pristojno službo Ministrstva za pravosodje pregledala ustreznost zakonskih podlag za obdelavo osebnih podatkov, ugotovila, kdo so upravljavci posameznih zbirk osebnih podatkov (posamezna ministrstva ali upravne enote?) ter pripravila enotne osnutke katalogov zbirk osebnih podatkov. Poleg tega bi bilo koristno, da bi prej navedena delovna skupina in Ministrstvo za javno upravo pripravila in izdala enoten pravilnik o zavarovanju osebnih

podatkov, ki bi veljal za vse upravne enote na področju Republike Slovenije.

## 4.2. **Pravosodje**

Na področju pravosodja se podobno kot na drugih področjih, nepravilnosti oziroma kršitve določb ZVOP kažejo predvsem v zvezi z vodenjem katalogov zbirk osebnih podatkov, posredovanjem podatkov iz katalogov za objavo v Registru zbirk osebnih podatkov, kjer je stanje popolnoma neurejeno in ne odraža dejanskega stanja. Poleg tega sodišča tudi nimajo izdelanih ustreznih notranjih aktov, v katerih bi bili predpisani organizacijski, tehnični in logično tehnični postopki in ukrepi za zavarovanje osebnih podatkov.

V obravnavanem obdobju smo v zvezi z obdelavo osebnih podatkov prejeli 2 pritožbi, ki sta bili vloženi zaradi suma nezakonitega zbiranja osebnih podatkov za namene vodenja sodnih postopkov. Obe pritožbi oziroma prijavi sta se sicer izkazali kot neutemeljeni, vendar pa moramo v zvezi z zbiranjem osebnih podatkov za namene vodenja sodnih postopkov opozoriti na, po našem mnenju, povsem neprimeren način zbiranja osebnih podatkov s strani sodišč. Kot primer takšnega neprimerne zbiranja osebnih podatkov s strani sodišča navajamo tekst, ki ga je eno od okrožnih sodišč v letu 2004 naslovilo na delodajalca ene od strank v pravnem postopku:

*»Zadeva: Poizvedba*

*Pri tukajšnjem sodišču je v teku pravdna zadeva tožeče stranke xx xx, xx, xxx, ki ga zastopa odvetnik xx xx, zoper toženo stranko xx xx, xx, xx, ki jo zastopa odvetnik xx xx zaradi razveze zakonske zveze v pridruženi zadevi P xxx zaradi dodelitve mld. otrok in plačila preživnine. Prosim vas, da nam v roku 5 dni pošljete podatke o netto OD za xx xx, za zadnje 3 mesece. Glavna obravnava je razpisana v predmetni zadevi za dne xx.xx.xxxx.«*

Sodišča imajo v 13. členu Zakona o sodiščih ter v procesnih zakonih (10. člen Zakona o pravnem postopku, 143. člen Zakona o kazenskem postopku, 4. člen Zakona o izvršbi in zavarovanju) sicer ustrezne zakonske podlage za zbiranje tistih osebnih podatkov, ki so sodišču potrebni za ugotovitev dejstev v zvezi z vodenim postopkom oziroma za odločitev o stvari, vendar pa je zgoraj citirano zaprosilo za posredovanje podatkov o plači z vidika določb Zakona o varstvu osebnih podatkov povsem neprimerno. Neprimerno je iz dveh razlogov, ki jih v nadaljevanju podrobneje pojasnjujemo.

**Prvič** je zaprosilo sporno iz razloga, ker v njem ni navedena zakonska podlaga, ki sodišče pooblašča za pridobivanje zahtevanih osebnih podatkov in bi po našem mnenju v zaprosilu morala biti navedena.

Po določbah tretjega odstavka 22. člena ZVOP-1, ki velja od 1. januarja 2005 dalje, mora upravljavec osebnih podatkov za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj **in na kakšni podlagi**, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov. Podobne določbe glede evidentiranja posredovanja osebnih podatkov so bile vsebovane tudi v petem odstavku 11. člena ZVOP, ki je veljal v času, ki je sodišče delodajalcu posredovalo zgoraj citirano zaprosilo.

Iz zgoraj citiranih določb ZVOP in ZVOP-1 izhaja, da mora delodajalec ob tem, ko sodišču posreduje podatke o višini plače, takšno posredovanje ustrezno evidentirati, in sicer na način,

da bo med drugim mogoče pozneje ugotoviti tudi to, **na kakšni podlagi** so bili osebni podatki posredovani sodišču. Takšno evidentiranje je potrebno iz razloga, ker je delodajalec kot upravljavec osebnih podatkov dolžan posamezniku, na katerega se podatki nanašajo, skladno z določbami 4. točke prvega odstavka 30. člena ZVOP-1 (18. člen ZVOP) med drugim posredovati tudi seznam uporabnikov osebnih podatkov, katerim so bili posredovani osebni podatki, kdaj, **na kakšni podlagi** in za kakšen namen.

Ker sodišče v svoji vlogi ni citiralo zakonske podlage, ki sodišče pooblašča zbirati zahtevane osebne podatke, bi moral delodajalec po našem mnenju od sodišča zahtevati dopolnitev vloge oziroma zaprosila za posredovanje osebnih podatkov, in sicer tako, da bi od sodišča zahteval, da v svoji dopolnjeni vlogi navede tudi določbo zakona, ki sodišče pooblašča pridobivati zahtevane podatke. Brez navedbe pravne podlage v zaprosilu oziroma zahtevku za posredovanje osebnih podatkov delodajalec ali pa kakšen drug upravljavec osebnih podatkov ne ve in ne more evidentirati, na kakšni pravni podlagi je sodišču posređoval določene osebne podatke.

**Drugič** je zgoraj citirano zaprosilo neprimerno tudi z vidika načela sorazmernosti, saj je sodišče v zaprosilu po našem mnenju delodajalcu sporočilo veliko več podatkov, kot bi jih bilo potrebno glede na namene, zaradi katere se pošilja takšno zaprosilo. Po našem mnenju se namreč s posredovanjem takšnih zaprosil nedvomno prekomerno posega v zasebnost strank v postopku, saj sodišče s takšno poizvedbo delodajalca povsem po nepotrebnem, pa tudi povsem neupravičeno, seznanja s postopkom, pri katerem mora biti javnost glede na določbe 407. člena Zakona o pravnem postopku izključena.

Po našem mnenju bi morala sodišča ob upoštevanju načela sorazmernosti (3. člen ZVOP-1) v svojih zaprosilih oziroma poizvedbah, ki jih posređujejo upravljavcem osebnih podatkov, navesti le osebno ime in naslov osebe, za katero zahtevajo osebne podatke (lahko tudi še EMŠO ali davčno številko), vrsto podatkov, ki jih potrebujejo, opr. številko zadeve ter predvsem citirati določbo zakona, ki jih pooblašča zbirati zahtevane osebne podatke, na pa, da upravljavca osebnih podatkov obširno seznanjajo z vrsto postopka, ki ga vodijo.

#### **4.3. Lokalna samouprava**

V zvezi z obdelavo osebnih podatkov je inšpektorat za varstvo osebnih podatkov v letu 2004 prejel eno pritožbo, ki je bila vložena zaradi suma nezakonite uporabe osebnih podatkov iz evidence prekrškov. Pri obravnavi prijave je bilo ugotovljeno, da organi lokalne uprave v letu 2004 sploh niso imeli pravne podlage za vodenje evidence o prekrških, zaradi česar je bila občini izdana odločba, s kateri ji je bil naložen izbris spornih podatkov. Pravno praznino v zvezi z vodenjem evidence prekrškov je razrešil novi Zakon o prekrških<sup>13</sup>, ki je stopil v veljavo s 1. januarjem 2005 in s katerim so občine in ostali prekrškovni organi dobili neposredno zakonsko podlago za vodenje Evidence o izdanih odločbah o prekrških.

Sicer pa na področju lokalne samouprave ugotavljamo, da večina občin za svoje zbirke osebnih podatkov še vedno ni zagotovila katalogov zbirk osebnih podatkov ter podatkov iz katalogov tudi še ni posređovala pristojnemu organu, ki vodi Register zbirk osebnih podatkov. Pri večini občin, ki so podatke iz svojih katalogov že posređovale Ministrstvu za pravosodje, je iz vpogleda v Register zbirk osebnih podatkov razvidno, da so podatki povsem zastareli in neažurni

---

<sup>13</sup> Uradni list RS. št. 7/03, 7/05, 34/05 in 44/05.

oziroma, da podatki ne odražajo dejanskega stanja.

Nepravilnosti oziroma pomanjkljivosti se kažejo tudi v zvezi z notranjimi akti, s katerimi morajo občine kot upravljalci osebnih podatkov predpisati organizacijske, tehnične in logično tehnične postopke in ukrepe za zavarovanje osebnih podatkov, saj veliko občin takšnih postopkov in ukrepov še vedno sploh nima predpisanih.

#### **4.4. Vzgoja in izobraževanje**

Pri opravljanju preventivnega nadzora in pri obravnavi prijav na področju vzgoje in izobraževanja so bile ugotovljene predvsem sledeče nepravilnosti:

- posamezne šole še vedno nimajo izdelanih katalogov zbirk osebnih podatkov ter podatkov iz katalogov še vedno niso posredovale Ministrstvu za pravosodje;
- še vedno se najdejo šole, ki v svojih notranjih aktih nimajo predpisanih organizacijskih in ustreznih logično tehničnih postopkov in ukrepov za zavarovanje osebnih podatkov;
- pisne privolitve posameznikov za zbiranje osebnih podatkov o učencih in dijakih, ki jih obravnava svetovalna služba, so pogosto pomanjkljive, saj iz njih ni dovolj jasno razviden namen obdelave in uporabe osebnih podatkov ter čas shranjevanja zbranih osebnih podatkov, poleg tega pa iz izjav oziroma pisnih privolitev v večini primerov tudi ni razvidno, katere vrste osebnih podatkov se bodo obdelovale;
- podatki o gibalnih sposobnostih in morfoloških značilnostih se pogosto zbirajo tudi od tistih učencev in dijakov, ki so na izjavi oziroma pisni privolitvi posameznika za zbiranje takšnih podatkov obkročili, da ne soglašajo s tem, da so v tekočem šolskem letu vključeni v spremljavo telesnega in gibalnega razvoja "ŠPORTNOVZGOJNI KARTON", kar dejansko pomeni nezakonito obdelavo osebnih podatkov;
- izrečeni vzgojni ukrepi so se v nekaterih šolah še vedno vpisovali v dnevnike, pogosti pa so tudi primeri, ko se dokumentacija v zvezi z izrečenimi vzgojnimi ukrepi ne uničuje v predpisanih rokih oziroma se o uničenju dokumentacije ne naredi ustreznih zapisnikov.

K zgoraj navedenemu moramo dodati, da se je stanje na področju vzgoje in izobraževanja v zadnjih letih kljub vsemu bistveno izboljšalo, kar je predvsem posledica opravljanja inšpekcijskega nadzora na tem področju, pa tudi aktivnosti, ki jih v zvezi s tem izvaja Ministrstvo za šolstvo in šport in njihov inšpektorat. Vendar pa je potrebno kljub temu pripomniti, da zakonodaja, ki ureja obdelavo osebnih podatkov na področju vzgoje in izobraževanja (Zakon o osnovni šoli, Zakon o gimnazijah, Zakon o poklicnem in strokovnem izobraževanju), še vedno ni povsem usklajena z določbami ZVOP. Kot primer navajamo izrekanje vzgojnih ukrepov, kjer je v podzakonskih aktih določeno, da se obvestila o izrečenih vzgojnih ukrepih hranijo v mapi vzgojnih ukrepov. Takšna mapa z vidika določb ZVOP nedvomno pomeni zbirko osebnih podatkov, za vodenje katere pa v zakonih, ki urejajo obdelavo osebnih podatkov na področju vzgoje in izobraževanja, ni zakonske podlage.

Pomanjkljivost se kaže tudi v zvezi z obdelavo osebnih podatkov o starših in skrbnikih mladoletnih dijakov, saj v Zakonu o gimnazijah ter v Zakonu o poklicnem in strokovnem izobraževanju ni nikjer določeno, da lahko poklicne in strokovne šole ter gimnazije obdelujejo tudi osebne podatke staršev mladoletnih dijakov. Navedeno pravno praznino so poklicne in strokovne šole ter gimnazije zapolnile na ta način, da si za obdelavo osebnih podatkov dijakovih staršev pridobijo pisno privolitev posameznika, kar pa je z vidika določb ZVOP precej sporno, saj lahko javni sektor praviloma obdeluje le tiste osebne podatke, za katere je tako določeno z zakonom (3. člen ZVOP in 9. člen ZVOP-1).

#### **4.5. Zdravstveno varstvo**

Na področju zdravstvenega varstva se nepravilnosti kažejo predvsem v zvezi z neustreznim zavarovanjem osebnih podatkov, ki bi glede na to, da podatki o zdravstvenem stanju spadajo v kategorijo tako imenovanih občutljivih osebnih podatkov, morali biti glede na določbe ZVOP še posebej označeni in zavarovani.

V praksi ugotavljamo, da je zavarovanje nosilcev z osebnimi podatki o zdravstvenem stanju posameznikov daleč od ustreznega. Vsi zdravstveni zavodi, v katerih se je opravljal inšpekcijski nadzor nad izvajanjem določb ZVOP, so sicer v svojih notranjih aktih že imeli predpisane organizacijske, tehnične in logično tehnične postopke in ukrepe za zavarovanje osebnih podatkov, vendar pa so bili ti akti glede na specifikko obdelave osebnih podatkov in glede na občutljivost podatkov, ki kažejo na zdravstveno stanje posameznika, v večini primerov precej pomanjkljivi.

Poleg pomanjkljivih aktov, ki določajo postopke in ukrepe za zavarovanje osebnih podatkov, je bilo ugotovljeno, da je tudi sama izvedba zavarovanja nosilcev z osebnimi podatki na tem področju daleč od ustrezne. Krog ljudi, ki ima dostop do bolnikove zdravstvene dokumentacije je po našem mnenju preširok, poleg tega pa se zdravstvena dokumentacija o bolnikih, ki ležijo na intenzivni negi, pogosto nahaja kar na obposteljnih mizicah. Pogosti so bili primeri, ko se temperaturni list (le ta vsebuje sledeče podatke pacienta: ime in priimek, datum rojstva, diagnozo v latinščini, temperaturo, diete, terapijo in preiskave) še vedno izobeša na bolnikovo posteljo.

Ob tem je potrebno opozoriti, da se v praksi še vedno dogaja, da se omare z zdravstvenimi kartotekami v nekaterih primerih nezaklenjene nahajajo kar na hodnikih ali v čakalnicah, kar je z vidika določb ZVOP nedopustno. V letu 2004 smo obravnavali en tak primer, v okviru katerega smo zoper odgovorne seveda tudi ustrezno ukrepali.

Glede tehničnega zavarovanja nosilcev občutljivih osebnih podatkov (to so vse vrste sredstev, na katerih so zapisani ali posneti podatki: listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofili, naprave za prenos podatkov, ipd) ZVOP in ZVOP-1 ne predpisujeta minimalnih tehničnih standardov, vendar pa je glede na občutljivost podatkov o zdravstvenem stanju mogoče šteti, da je nosilce z občutljivimi osebnimi podatki potrebno hraniti v zaklenjenih ognjavnih omarah, prostore, kjer se takšne omare nahajajo, pa bi bilo koristno, če ne celo nujno, dodatno zavarovati še z videonadzornim sistemom, alarmno javljalno napravo ter protipožarno zaščito.

Ker ZVOP in ZVOP-1 ne predpisujeta minimalnih tehničnih standardov za zavarovanje podatkov o zdravstvenem stanju, je v 7. členu Zakona o zbirkah podatkov s področja zdravstvenega varstva<sup>14</sup> določeno, da minister, pristojen za zdravstvo, v soglasju z ministrom, pristojnim za pravosodje in ministrom, pristojnim za znanost in tehnologijo, predpiše tehnične in organizacijske ukrepe za zavarovanje podatkov v zbirkah podatkov, ki jih vodijo zdravstveni zavodi. Vendar pa takšen predpis še vedno ni izdan, zaradi česar Inšpektorat za varstvo osebnih podatkov meni, da je precejšen del krivde v zvezi z neustreznim zavarovanjem

---

<sup>14</sup> Uradni list RS, št. 65/2000.



podatkov o zdravstvenem stanju potrebno pripisati tudi Ministrstvu za zdravje.

Na področju zdravstvenega varstva se precej nepravilnosti in dilem pojavlja tudi v zvezi s posredovanjem informacij o bivanju pacienta v posamezni bolnišnici, v zvezi s posredovanjem podatkov o zdravstvenem stanju drugim osebam, v zvezi s pravicami posameznika do vpogleda, prepisa in izpisa podatkov, ki se nanašajo nanj ter v zvezi z varstvom osebnih podatkov umrlih. Ker gre v tem primeru za obdelavo zelo občutljivih osebnih podatkov, podajamo v nadaljevanju podrobnejša pojasnila v zvezi z navedeno problematiko.

V praksi ugotavljamo da so se v posameznih primerih informacije o bivanju pacienta v posamezni bolnišnici posredovale drugim osebam tudi prek telefona, pri čemer se ni vodila nobena evidenca, iz katere bi bilo razvidno, komu so bili posamezni osebni podatki posredovani. Tudi zdravniki, ki so bolnika zdravili in so z bolnikovim zdravstvenim stanjem seznanjali bolnikovega ožjega sorodnika ali skrbnika, takšnega posredovanja podatkov niso evidentirali.

Ko zdravstveni zavodi v praksi odločajo o posredovanju osebnih podatkov o zdravstvenem stanju drugim subjektom, morajo nujno upoštevati predvsem določbe Zakona o zdravstveni dejavnosti<sup>15</sup> ter določbe Zakona o zdravniški službi<sup>16</sup>.

Po določbah 47. člena Zakona o zdravstveni dejavnosti ima vsakdo pravico zahtevati, da zdravstveni delavci in njihovi sodelavci brez njegove izrecne privolitve nikomur ne posredujejo podatkov o njegovem zdravstvenem stanju. V primeru, da je posameznik podal takšno prepoved, je po našem mnenju z vidika določb Zakona o varstvu osebnih podatkov dopustno podatke o njegovem zdravstvenem stanju posredovati le v dveh izjemnih primerih, in sicer na podlagi izrecne in utemeljene odredbe sodišča ali pa v primeru, če je posredovanje osebnih podatkov nujno potrebno za varovanje življenja in telesa posameznika, na katerega se podatki nanašajo.

Pri odločanju glede posredovanja podatkov o zdravstvenem stanju drugim subjektom je potrebno vedno upoštevati tudi določbe 51. člena Zakona o zdravstveni dejavnosti, kjer je določena dolžnost varovanja poklicne skrivnosti. Iz navedenih določb izhaja, da se podatki o zdravstvenem stanju posameznika in o vzrokih, okoliščinah in posledicah tega stanja ne smejo dajati drugim ljudem oziroma javnosti in tudi ne objavljati na način, ki bi omogočal razkritje posameznika, na katerega se nanašajo. Dolžnosti varovanja poklicne skrivnosti lahko zdravstvenega delavca ali zdravstvenega sodelavca razreši prizadeta oseba sama ali sodišče, za mladoletne osebe in za osebe pod skrbništvom pa starši oziroma skrbniki. Podobne določbe so tudi v 51. in 52. členu Zakona o zdravniški službi.

Zgoraj omenjene določbe glede dolžnosti varovanja poklicne skrivnosti po našem mnenju v ničemer ne omejujejo izmenjave oziroma zbiranja osebnih podatkov na način, kot je to dokaj natančno določeno v Prilogi Zakona o zbirkah podatkov s področja zdravstvenega varstva, pač pa določbe glede dolžnosti varovanja poklicne skrivnosti omejujejo predvsem posredovanje podatkov o zdravstvenem stanju tistim uporabnikom, ki za uporabo podatkov niso izrecno pooblaščen z Zakonom o zbirkah podatkov s področja zdravstvenega varstva ali kakšnim drugim zakonom. Prav tako določbe glede varovanja poklicne skrivnosti tudi ne

---

<sup>15</sup> Uradni list RS, št. 9/92 s spremembami in dopolnitvami.

<sup>16</sup> Uradni list RS, št. 98/99.

bodo več omejevale uporabe podatkov o zdravstvenem stanju za namene strokovnega nadzora, saj zakonska podlaga za uporabo osebnih podatkov za namene strokovnega nadzora zdaj izhaja neposredno iz določb 87., 88., 89. in 90. člena ZVOP-1, pri čemer je seveda pomembno, da se osebni podatki obdelujejo v skladu s prej navedenimi določbami. Problem v zvezi z uporabo osebnih podatkov za namene strokovnega nadzora bo lahko nastal le v primeru, ko bo posameznik podal prepoved iz sedme alineje 47. člena Zakona o zdravstveni dejavnosti.

Kot izhaja iz določb 53. člena Zakona o zdravniški službi ter določb 51. člena Zakona o zdravstveni dejavnosti, lahko brez predhodnega soglasja bolnika podatke o bolnikovem zdravstvenem stanju ter podatke o vzrokih, okoliščinah in posledicah tega stanja daje bolnikovim ožjim sorodnikom ali skrbnikom oziroma izvenzakonskemu partnerju le zdravnik, ki bolnika zdravi, če oceni, da je to v bolnikovo korist. Ob tem je potrebno opozoriti, da takšno posredovanje ni dopustno, če je posameznik podal prepoved iz 47. člena Zakona o zdravstveni dejavnosti ter, da je potrebno tudi za vsako sporočanje podatkov ožjim sorodnikom zagotoviti, da bo mogoče pozneje ugotoviti, kateri podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Glede pravice bolnika, da prepove posredovanje podatkov o zdravstvenem stanju drugim osebam, glede posredovanja podatkov o zdravstvenem stanju ožjim sorodnikom ter glede pravice bolnika do vpogleda v svojo zdravstveno dokumentacijo je mogoče več prebrati v Odločbi o ugotovitvi neskladnosti določb 70. in 81. člena Zakona o nepravdnem postopku z Ustavo in o ugotovitvi skladnosti šeste alineje 47. člena, 48. člena, prvega odstavka 49. člena in četrtega odstavka 51. člena Zakona o zdravstveni dejavnosti<sup>17</sup>.

V zvezi s sporočanjem podatkov o bivanju pacienta v posamezni bolnišnici je bilo ugotovljeno, da je bila v bolnišnicah (v preteklosti?) praksa, da so informatorji v bolnišnicah podatke o tem, kdo leži v bolnišnici ter na katerem oddelku leži posamezni pacient, posredovali katerikoli osebi, pogosto tudi kar preko telefona. Pri takšnem posredovanju podatkov se ni beležilo, komu so bili posredovani takšni podatki, poleg tega pa informator niti ni ugotavljal identitete kličočega ali druge osebe, ki se je zanimala za podatke o zdravstvenem stanju pacienta. Ob sprejemu pacienta v bolnišnico so pacienti podpisovali le dovoljenje za posege v telo in anestezijo, niso pa podpisovali nobene izjave, ki bi jo bilo mogoče šteti kot pisno privolitev posameznika za sporočanje njegovih osebnih podatkov drugim osebam, npr. sorodnikom in podobno.

Zgoraj opisano ravnanje bolnišnic je v nasprotju zlasti z določili 8., 9., 16. in 22. člena ZVOP-1 (3., 9. in 11. člen ZVOP) ter 53. člena Zakona o zdravniški službi. Iz podatka o tem, na katerem oddelku neke bolnišnice se z osebnim imenom določeni posameznik nahaja, je namreč že mogoče sklepati o njegovem zdravstvenem stanju, pa tudi o posledicah tega stanja, zato v primeru posredovanja oziroma obdelave teh podatkov že lahko govorimo o obdelavi osebnih podatkov, ki bi morala biti glede na občutljivost skladno z določbami 14. člena ZVOP-1 še posebej označena in zavarovana.

Po opozorilu inšpektorata so v nekaterih bolnišnicah pripravili obrazce izjav oziroma pisnih privolitev posameznika, s katerimi so pacientom dali možnost, da se ob sprejemu v bolnišnico sami odločijo ob tem, komu bolnišnica lahko posreduje podatke o njegovem bivanju v bolnišnici ter komu pacient dovoljuje obiske. Takšne obrazce dobijo v podpis vsi pacienti, razen tistih, ki ob sprejemu v bolnišnico (npr. na urgenco) niso v stanju podpisati takšne izjave. V takšnih

---

<sup>17</sup> Odločba Ustavnega sodišča, Uradni list RS, št. 131/2003.

primerih je posredovanje podatkov na podlagi 51. člena Zakona o zdravstveni dejavnosti in 53. člena Zakona o zdravniški službi dovoljeno le ožjim sorodnikom, pri čemer je vsako takšno posredovanje seveda potrebno tudi evidentirati, kot je to določeno v tretjem odstavku 22. člena ZVOP-1.

V praksi se veliko nepravilnosti in dilem pojavlja tudi v zvezi z uresničevanjem pravice posameznika, da vpogleda v svojo zdravstveno dokumentacijo oziroma, da si pridobi kopije svoje zdravstvene dokumentacije ali pridobi izpis podatkov, ki se nanašajo nanj. V takšnih primerih je zdaj potrebno dosledno upoštevati določbe 30. in 31. člena ZVOP-1<sup>18</sup> kar pomeni, da je potrebno v zakonsko določenem roku (15 ali 30 dni) posamezniku bodisi omogočiti vpogled, prepis, kopiranje oziroma mu posredovati izpis podatkov, ki se nanašajo nanj, ali pa mu v istem roku posredovati pisno pojasnilo o razlogih, zaradi katerega mu to ne bo omogočeno. Pravice posameznika iz 30. člena ZVOP-1 je glede na določbe 36. člena ZVOP-1 ter določbe šeste alineje 47. člena Zakona o zdravstveni dejavnosti mogoče omejiti le v izjemnih primerih, pri čemer opozarjamo, da je glede na razlago Ustavnega sodišča Republike Slovenije<sup>19</sup> zdravnik bolniku na njegovo zahtevo praviloma dolžan vedno in brez pogojevanja omogočiti vpogled v vse njegove objektivne in izvirne medicinske podatke (npr. v laboratorijske in rentgenske izvide), poleg tega pa omogočiti tudi prenos (prepis) teh podatkov. V izjemnih primerih zdravnik lahko omeji ali prepreči vpogled v svoje osebne zapiske in ocene v dokumentaciji, katerih razkritje bi lahko hudo motilo proces zdravljenja ali razmerje med bolnikom in zdravnikom, bolnik pa lahko v takšnih primerih svojo pravico do vpogleda v medicinsko dokumentacijo uveljavlja po sodni poti (v upravnem sporu na podlagi 34. člena ZVOP-1).

V zvezi z uresničevanjem pravice državljanov do vpogleda v zdravstvene podatke je potrebno opozoriti, da minister, pristojen za zdravje še vedno ni predpisal postopka, kako lahko posamezni državljan uresničuje pravico do vpogleda v osebne zdravstvene podatke, kot to določa 8. člen Zakona o zbirkah podatkov s področja zdravstvenega varstva.

V praksi se je v obravnavanem obdobju pojavljalo tudi precej dilem glede posredovanja osebnih podatkov, ki se nanašajo na umrle. Varstvo osebnih podatkov umrlih je sedaj na splošno urejeno v določbah 23. člena ZVOP-1<sup>20</sup>. Po določbi prvega odstavka 23. člena lahko upravljavec osebnih podatkov podatke o umrlem posamezniku posreduje samo tistim uporabnikom osebnih podatkov, ki so za obdelavo osebnih podatkov pooblašteni z zakonom.

Osebni podatki o umrlem posamezniku se lahko posredujejo tudi osebi, ki je po zakonu, ki ureja dedovanje, njegov zakoniti dedič prvega ali drugega dednega reda (otroci, zakonec in starši), če za uporabo osebnih podatkov izkaže pravni interes, umrli posameznik pa ni pisno prepovedal posredovanja teh osebnih podatkov. ZVOP-1 torej v svojem 23. členu po eni strani daje zakonitim dedičem prvega in drugega dednega reda neposredno pravno podlago, da ob izpolnitvi dveh kumulativnih pogojev pridobijo osebne podatke o umrlem posamezniku, po drugi strani pa živečim posameznikom daje tudi možnost, da še za časa svojega življenja prepovedo vsakršno posredovanje svojih osebnih podatkov po svoji smrti. Če je posameznik v času svojega življenja podal takšno prepoved, je po našem mnenju dopustno njegove osebne podatke po njegovi smrti posredovati le tistim uporabnikom osebnih podatkov, ki

---

<sup>18</sup> V letu 2004 je to področje urejal 19. člen ZVOP.

<sup>19</sup> Odločba Ustavnega sodišča Republike Slovenije št. U-I-60/03-20, Uradni list RS, št. 131/2003.

<sup>20</sup> V letu 2004 je to področje urejal 12. člen ZVOP.

imajo za pridobivanje takšnih osebnih podatkov izrecno podlago v zakonu.

Kot že rečeno, morata biti za posredovanje osebnih podatkov zakonitemu dediču prvega ali drugega dednega reda izpolnjena dva kumulativna pogoja, in sicer zakoniti dedič mora izkazati pravni interes, drugi pogoj pa je ta, da umrli posameznik v času svojega življenja posredovanja svojih osebnih podatkov ni pisno prepovedal. Pravni interes za pridobivanje osebnih podatkov o umrlem je lahko po našem mnenju izkazan le v primeru, če zakoniti dedič podatke o umrlem posamezniku potrebuje zaradi varovanja ali uveljavljanja svojih pravic pred osebami javnega sektorja, kar pomeni, da mora v svoji vlogi za pridobitev osebnih podatkov umrlega jasno navesti, kakšne svoje pravice bo varoval oziroma uveljavljal ter pred katerimi osebami javnega sektorja bo te svoje pravice varoval oziroma uveljavljal.

Če zakon ne določa drugače, lahko upravljavec osebnih podatkov podatke o umrlem posamezniku posreduje tudi katerikoli drugi osebi, ki namerava te podatke uporabljati za zgodovinsko, statistično ali znanstveno-raziskovalne namene, če umrli posameznik ni pisno prepovedal posredovanja teh osebnih podatkov. V primeru pridobivanja in obdelave osebnih podatkov na tej pravni podlagi je potrebno postopati v skladu z določbami 17. člena ZVOP-1, v katerem so predpisana pravila glede obdelave osebnih podatkov za zgodovinsko, statistično in znanstveno-raziskovalne namene. To pomeni, da je potrebno rezultate raziskave objaviti v anonimizirani obliki ter, da se morajo osebni podatki ob zaključku obdelave uničiti, uporabnik osebnih podatkov pa mora upravljavca osebnih podatkov brez odlašanja obvestiti, kdaj in na kakšen način je podatke uničil.

Če umrli posameznik ni podal prepovedi posredovanja osebnih podatkov za zgodovinsko, statistično ali znanstveno-raziskovalne namene, lahko osebe, ki so po zakonu, ki ureja dedovanje, njegovi zakoniti dediči prvega ali drugega dednega reda, pisno prepovejo posredovanje njegovih podatkov, če zakon ne določa drugače. Skladno s takšno določbo lahko zakoniti dediči prvega in drugega dednega reda kadar koli prepovedo posredovanje osebnih podatkov za zgodovinsko, statistično ali znanstveno-raziskovalne namene.

Ker gre do pravice iz drugega in četrtega odstavka 23. člena ZVOP-1 glede obdelave osebnih podatkov o umrlih le zakonitem dedičem prvega ali drugega dednega reda, bo mora zakoniti dedič k svoji zahtevi, s katero bo uveljavljal katero od teh svojih pravic, priložiti tudi dokaz, iz katerega bo razvidno, da je oseba, ki zahteva osebne podatke o umrlem, res njegov zakoniti dedič. To pomeni, da bo moral zakoniti dedič k svoji zahtevi priložiti ali dati na vpogled npr. izpisek oziroma potrdilo iz matičnega registra, poročni list, ali drug ustrezen dokument.

V zvezi z obdelavo občutljivih osebnih podatkov, ki se nanašajo na umrle, je potrebno posebej opozoriti tudi na omejitve, ki jih v zvezi z obdelavo takšnih osebnih podatkov predpisuje že sam ZVOP-1. ZVOP-1 namreč v 13. členu taksativno določa 8 primerov, v katerih je občutljive osebne podatke sploh dovoljeno obdelovati. Navedeno pomeni, da je v primeru, ko zakoniti dediči prvega ali drugega dednega reda ali kdorkoli drug, sklicujoč se na 23. člen ZVOP-1, zahteva posredovanje občutljivih osebnih podatkov o umrlem, mora upravljavec osebnih podatkov pred posredovanjem takšnih podatkov obvezno preveriti, če je za posredovanje osebnih podatkov izpolnjen kateri od pogojev, ki jih v zvezi s tem predpisuje 13. člen ZVOP-1.

#### **4.6. Delovne evidence in obdelava osebnih podatkov zaposlenih**

Na področju vodenja delovnih evidenc ter obdelave osebnih podatkov zaposlenih je podobno kot na drugih področjih ugotovljeno največ nepravilnosti v zvezi s katalogi zbirk osebnih podatkov ter v zvezi z notranjimi akti, ki določajo postopke in ukrepe za zavarovanje osebnih podatkov.

V obravnavanem obdobju so bile v zvezi z obdelavo osebnih podatkov zaposlenih vložene pritožbe predvsem zaradi suma prekomernega zbiranja osebnih podatkov o zaposlenih in kandidatih za zaposlitev, zaradi suma neustreznega zavarovanja osebnih podatkov ter zaradi izvajanja videonadzora.

V zvezi z vodenjem delovnih evidenc in obdelavo osebnih podatkov zaposlenih je potrebno na tem mestu opozoriti predvsem na to, da je zakonodaja, ki ureja navedeno področje, že zdavnaj zastarela, saj je še vedno v veljavi Zakon o evidencah na področju dela (Uradni list SFRJ, št. 17/90), ki je bil sprejet še v bivši Jugoslaviji. Zaradi tega bo moralo pristojno ministrstvo po našem mnenju čimprej sprejeti nov, sodobnejši zakon, ki bo predpisoval delovne evidence oziroma natančneje urejal obdelavo osebnih podatkov zaposlenih.

V obravnavanem obdobju se je inšpektorat precej ukvarjal s problematiko videonadzora v delovnih prostorih. Navedeno področje je bilo v obravnavanem obdobju pomanjkljivo pravno urejeno, zaradi česar so se kot pravna podlaga za upravljanje videonadzora lahko uporabljale le določbe Zakona o zasebnem varovanju<sup>21</sup>, v katerem pa je bilo področje videonadzora ter predvsem razlogi za njegovo uvedbo pomanjkljivo urejeno. Pravno praznino na tem področju je zapolnil šele ZVOP-1, ki v členih 74. do 77. sicer dokaj natančno ureja področje videonadzora, vendar pa so se določbe navedenega zakona pričele uporabljati šele s 1. januarjem 2005. Zaradi tega bi morali delodajalci do navedenega datuma bodisi uskladiti izvajanje videonadzora z določbami ZVOP-1, ali pa prenehati opravljati videonadzor.

V zvezi z videonadzorom je potrebno opozoriti, da nekateri delodajalci težijo k temu, da bi videonadzor v delovnih prostorih namestili izključno zaradi kontrole izrabe delovnega časa. Takšen videonadzor je po našem mnenju nezakonit in nedopusten, saj pretirano oziroma nesorazmerno posega v zasebnost zaposlenih. Izvajanje videonadzora znotraj delovnih prostorov je namreč z vidika določb 77. člena ZVOP-1 dopustno le v izjemnih primerih, to je takrat, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, pa tega namena ni mogoče doseči z milejšimi ukrepi. Navedeno pomeni, da bo moral delodajalec, ki se bo odločil za videonadzor delovnih prostorov, za vsako nameščeno kamero obrazložiti, zakaj je namestitev kamere oziroma izvajanje videonadzora v določenem prostoru nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti.

---

<sup>21</sup> Uradni list RS, št. 126/2003.

## **5. SPLOŠNA OCENA STANJA NA PODROČJU VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI**

Ugotovitve Inšpektorata za varstvo osebnih podatkov kažejo, da se stanje na področju varstva osebnih podatkov v zadnjih letih sicer precej izboljšuje, vendar pa stanje še vedno ni takšno, kot bi po našem mnenju moralo biti. Nepravilnosti oziroma kršitve, ki smo jih ugotovili v obravnavanem obdobju, po naših ugotovitvah v večini primerov niso bile posledica namernega kršenja določb ZVOP, pač pa so ugotovljene nepravilnosti v prvi vrsti posledica tega, da upravljavci osebnih podatkov bodisi slabo poznajo določbe Zakona o varstvu osebnih podatkov, ali pa varstvu osebnih podatkov posvečajo bistveno premalo pozornosti.

Najpogosteje ugotovljene nepravilnosti oziroma kršitve varstva osebnih podatkov v Republiki Sloveniji, ki jih predstavljamo v nadaljevanju, so bolj ali manj podobne nepravilnostim oziroma kršitvam iz preteklih let. Kot že rečeno, najpogosteje ugotovljene nepravilnosti oziroma kršitve so mnogokrat posledica nepoznavanja, pa tudi nerazumevanja posameznih določb Zakona o varstvu osebnih podatkov. Zaradi tega smo zaradi vprašanj oziroma nejasnosti, ki se v praksi pogosto zastavljajo upravljavcem osebnih podatkov, k opisu najpogosteje ugotovljenih nepravilnosti, dodali tudi nekaj pojasnil in priporočil, za katere upamo, da bodo razjasnila nekatere dileme ter prispevala k izboljšanju stanja oziroma odpravi najpogosteje ugotovljenih nepravilnosti.

### **5.1. Nepravilnosti v zvezi s katalogi zbirk osebnih podatkov ter registrom zbirk osebnih podatkov**

Kot je razvidno iz pregleda stanja po posameznih področjih, so najpogosteje ugotovljene nepravilnosti na področju varstva osebnih podatkov še vedno nepravilnosti v zvezi s katalogi zbirk osebnih podatkov (15. člen ZVOP) ter nepravilnosti v zvezi s posredovanjem podatkov iz katalogov Ministrstvu za pravosodje (16. člen ZVOP), kar se v praksi kaže v tem, da večina upravljavcev osebnih podatkov tega področja sploh še nima urejenega.

Stanje na tem področju se sicer iz leta v leto izboljšuje, kljub temu pa ugotavljamo, da je izboljšanje stanja v zvezi z vodenjem katalogov zbirk osebnih podatkov še vedno v prvi vrsti posledica inšpekcijskih ukrepov, s katerimi se upravljavce zbirk osebnih podatkov prisili k ureditvi zadeve.

ZVOP-1, ki je stopil v veljavo s 1. januarjem 2005, se v določbah, ki predpisujejo vodenje katalogov zbirk osebnih podatkov ter vodenje Registra zbirk osebnih podatkov (26., 27. in 28. člen ZVOP-1), precej razlikuje od zakona, ki je veljal v letu 2004. Zaradi teh sprememb bodo morali vsi upravljavci osebnih podatkov kataloge zbirk osebnih podatkov uskladiti z določbami novega zakona. Poleg tega bodo morali upravljavci osebnih podatkov, ki so podatke iz svojih katalogov posredovali še po določbah starega zakona (ZVOP), upravljavcu Registra zbirk osebnih podatkov do 02.04.2006 posredovati še vse manjkajoče podatke<sup>22</sup>.

---

<sup>22</sup> Po določbah 16. člena ZVOP so morali upravljavci osebnih podatkov organu, ki vodi Register zbirk osebnih podatkov (po določbah ZVOP se je zdajšnji Register zbirk osebnih podatkov imenoval Skupni katalog osebnih podatkov), iz svojih katalogov posredovati le sledeče podatke: 1. naziv zbirke osebnih podatkov; 2. podatke o upravljavcu osebnih podatkov; 3. kategorije posameznikov, na katere se nanašajo podatki v posamezni zbirki; ter 4. vrste osebnih podatkov, ki so shranjeni v posamezni zbirki. Vsi upravljavci, ki so prej naštetih podatke že posredovali organu, ki vodi Register zbirk osebnih podatkov, mu bodo sedaj morali do 02.04.2006 za vsako zbirko osebnih podatkov posredovati še sledeče podatke: 5. namen obdelave; 6. uporabniki ali kategorije

Da bi razjasnili nejasnosti v zvezi z dolžnostjo vodenja katalogov zbirk osebnih podatkov ter, da bi upravljavcem osebnih podatkov olajšali pripravo katalogov zbirk osebnih podatkov in posredovanje podatkov iz katalogov organu, ki vodi Register zbirk osebnih podatkov, je Ministrstvo za pravosodje v sodelovanju z Inšpektoratom za varstvo osebnih podatkov pripravilo in na svojih spletnih straneh objavilo podrobnejša pojasnila v zvezi s tem ter hkrati objavilo tudi nekatere vzorce katalogov zbirk osebnih podatkov. Objavljena pojasnila in vzorci so seveda že pripravljene v skladu z določbami ZVOP-1 in določbami Pravilnika o metodologiji vodenja registra zbirk osebnih podatkov<sup>23</sup> ter bodo po našem mnenju upravljavcem osebnih podatkov lahko služili kot koristen pripomoček pri izpolnitvi zahtev, ki jim jih nalaga ZVOP-1.

## **5.2. Nepravilnosti v zvezi z neustreznim zavarovanjem osebnih podatkov ter novosti, ki jih prinaša novi ZVOP-1**

Nepravilnosti na področju varstva osebnih podatkov se še vedno pre pogosto kažejo v pomanjkljivih notranjih aktih, v katerih so morali upravljavci osebnih podatkov skladno z določbami 13. in 14. člena ZVOP predpisati organizacijske in ustrezne logično tehnične postopke in ukrepe za zavarovanje osebnih podatkov. V zvezi s tem se pogosto dogaja, da posamezni upravljavci osebnih podatkov takšnih aktov še vedno sploh niso izdali, pogosti pa so tudi primeri, ko so postopki in ukrepi za zavarovanje osebnih podatkov sicer predpisani, vendar pa osebe, ki obdelujejo osebne podatke, z takšnimi akti sploh niso seznanjene.

Pogosti so tudi primeri, ko upravljavci osebnih podatkov ne zagotovijo ustreznega zavarovanja osebnih podatkov oziroma ne izvajajo v svojih notranjih aktih predpisanih postopkov in ukrepov za zavarovanje osebnih podatkov. Najpogostejši primeri neustreznega zavarovanja osebnih podatkov, ki so bili v preteklosti odkriti pri opravljanju inšpekcijskega nadzora, so predvsem:

- Neustrezno hranjenje dokumentacije, ki vsebuje osebne podatke: dokumentacija, se nahaja v nezaklenjenih omarah, ki se pogosto nahajajo kar na hodnikih.
- Neustrezno varovani prostori, v katerih se nahajajo nosilci osebnih podatkov ter računalniška oprema, s katero se obdelujejo osebni podatki. V zvezi s tem je potrebno upravljavce osebnih podatkov opomniti, da zbirk osebnih podatkov ter drugih občutljivih podatkov ni primerno hraniti na osebnih računalnikih, še zlasti ne na prenosnikih, ki se nahajajo v posameznih pisarnah. Obstaja namreč možnost, da nepridipravi skupaj z računalnikom odnesejo tudi osebne ali druge zaupne podatke, kot se je to zgodilo na eni od ameriških univerz. Po pisanju Računalniških novic je namreč neznanecu sredi belega dne iz slabo varovanih prostorov univerze uspelo odnesti prenosnik, na katerem so bili shranjeni osebni podatki (imena in priimki, naslovi, kraji rojstva, številke zavarovalnih polic, itd.) več kot 100.000 oseb, to je študentov, diplomantov, profesorjev ter drugih ljudi, povezanih z univerzo.
- Prenos oziroma pošiljanje dokumentacije, ki vsebuje osebne podatke, v prosojnih ali neustrezno zlepljenih ovojnica.
- Računalniško vodene zbirke osebnih podatkov niso varovane z gesli za identifikacijo in avtorizacijo oseb, ki obdelujejo osebne podatke. V zvezi s tem je potrebno upravljavce

---

uporabnikov osebnih podatkov; 7. dejstvo, ali se osebni podatki iznašajo v tretje države, kam, komu in pravno podlago iznosa; 8. splošen opis zavarovanja osebnih podatkov; 9. podatke o povezanih zbirkah osebnih podatkov iz uradnih evidenc in javnih knjig; ter 10. podatke o morebitnem zastopniku iz tretjega odstavka 5. člena ZVOP-1.

<sup>23</sup> Uradni list RS, št. 28/05.

osebnih podatkov opomniti, da so v praksi bili tudi primeri, ko so posamezne zbirke osebnih podatkov sicer bile varovane z vstopnimi gesli, vendar pa so zaposleni kot gesla uporabljali kar svoje ime, ki je bilo seveda napisano tudi na vratih njihove pisarne, ali pa so bila vstopna gesla napisana na lističih, ki so bili nalepljeni na računalniki ali omarah.

- Ni zagotovljena sledljivost obdelave osebnih podatkov oziroma sistem zavarovanja osebnih podatkov ne omogoča možnosti naknadnega ugotavljanja kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani ter kdo je to storil.
- Neustrezno zavarovanje osebnih podatkov pri uničevanju dokumentacije z osebnimi podatki ter nepopolno in malomarno uničevanje nosilcev z osebnimi podatki. Zasedili smo tudi primer, ko je bil osebni računalnik, na katerem so se hranili izredno občutljivi osebni podatki, predan drugemu uporabniku, ne da bi bivši uporabnik ali odgovorni poskrbeli, da bi se iz tega računalnika pred oddajo drugemu uporabniku izbrisali vsi osebni podatki.

V zvezi z zavarovanjem osebnih podatkov je v ZVOP-1 kar nekaj pomembnih novosti, katere bomo v nadaljevanju zaradi prepogosto ugotovljenih nepravilnosti ter pomena učinkovitega zavarovanja osebnih podatkov podrobneje opozorili.

Ena od novosti, ki jih v zvezi za zavarovanjem osebnih podatkov uvaja ZVOP-1, se kaže v tem, da ZVOP-1 v 24. členu zdaj izrecno določa, da so funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.

Pomembna novost, ki jo uvaja ZVOP-1 v svojem 25. členu je tudi ta, da morajo upravljavci osebnih podatkov poleg predpisovanja postopkov in ukrepov za zavarovanje osebnih podatkov, v svojih aktih zdaj določiti tudi osebe, ki so odgovorne za določene zbirke osebnih podatkov ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke. Navedeno pomeni, da je predstojnik upravljavca osebnih podatkov tisti, ki določa, katere osebe, ki so zaposlene pri upravljavcu osebnih podatkov, lahko obdeluje določene osebne podatke. Predstojnik mora pri tem upoštevati, da lahko posamezne osebne podatke pri upravljavcu osebnih podatkov obdelujejo le tiste osebe, ki osebne podatke nujno potrebujejo zaradi narave njihovega dela.

V notranjih aktih upravljavcev osebnih podatkov predpisani organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov morajo v prvi vrsti preprečiti nepooblaščen obdelavo osebnih podatkov, poleg tega pa morajo preprečiti tudi slučajno ali namerno nepooblaščen uničevanje podatkov ter njihovo spremembo ali izgubo. Da bi to dosegli, je potrebno v notranjih aktih predpisati, kako se:

1. varujejo prostori, oprema in sistemska programska oprema, vključno z vzhodno-izhodnimi enotami;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih omrežjih;
4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
5. omogoča poznejše ugotavljanje, kdaj so bili posamezni podatki uporabljeni ali vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega



posredovanja ali obdelave osebnih podatkov.

V zvezi z zgoraj navedenim velja opozoriti na 4. točko, ki je novost glede na stari zakon. Po tej določbi je namreč v notranjih aktih upravljavcev osebnih podatkov ter pogodbenih obdelovalcev zdaj potrebno predpisati tudi učinkovit način blokiranja, uničevanja, izbrisa ali anonimiziranja osebnih podatkov, hkrati pa je seveda potrebno zagotoviti tudi izvajanje predpisanih postopkov in ukrepov. Takšna določba je bila potrebna iz razloga, ker se je v praksi vse prepogosto dogajalo, da so se nosilci z osebnimi podatki pojavljali v koših za smeti ali na deponijah odpadnega papirja.

Notranji akti za zavarovanje osebnih podatkov so lahko samostojni akti ali pa akti v sklopu varovanja vseh zaupnih podatkov v neki ustanovi. Poleg splošnega akta je v specifičnih primerih priporočljivo izdelati še več izvedbenih aktov, ki podrobneje predpisujejo zavarovanje na posameznem področju (npr. navodilo za delo varnostnika, hišni red, podroben način preverjanja prisotnosti virusov, podroben predpis izdelave vsakodnevnih kopij mrežnih strežnikov, podrobnejše navodilo glede varovanja videonadzornega sistema ali sistema, s katerim se obdelujejo biometrični podatki, ipd.). Ob tem velja opozoriti, da mora biti splošen opis zavarovanja osebnih podatkov razviden že iz 11. točke kataloga zbirke osebnih podatkov, vendar pa je potrebno pri tem paziti, da takšen opis glede na to, da se podatki iz kataloga zbirk osebnih podatkov javno objavijo, ne bo služil kot pripomoček osebam, ki si želijo nezakonito priložiti osebne podatke.

### **5.3. Nepravilnosti in dileme, ki se pojavljajo v zvezi s pogodbeno obdelavo osebnih podatkov**

Upravljavec osebnih podatkov lahko skladno z določbami 7. člena ZVOP ter določbami 11. člena novega ZVOP-1 posamezna opravila v zvezi z obdelavo osebnih podatkov poveri drugi pravni ali fizični osebi, ki je registrirana za opravljanje takšne dejavnosti (pogodbenemu obdelovalcu). Ob tem moramo opozoriti, da med opravljanjem inšpekcijskega nadzora prepogosto ugotavljamo, da so takšne pogodbe z vidika določb 7. člena ZVOP oziroma določb 11. člena novega ZVOP-1 zelo pomanjkljive oziroma neustrezne. Zelo redke so namreč pogodbe, v katerih bi bila dovolj jasno določena naročnikova pooblastila pogodbenemu obdelovalcu v zvezi z obdelavo osebnih podatkov. Še redkejše pa so pogodbe, v katerih bi bili jasno določeni pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

Glede na to, da je v praksi večina pogodb s pogodbenimi obdelovalci pomanjkljivih in neustreznih, podajamo v nadaljevanju nekaj pojasnil in navodil, ki jih morajo upravljavci osebnih podatkov upoštevati pri sklepanju pogodb s pogodbenimi obdelovalci.

Kot že rečeno, ZVOP-1 podobno kot stari ZVOP, upravljavcu osebnih podatkov omogoča, da posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo poveri drugi pravni ali fizični osebi (pogodbenemu obdelovalcu), pri čemer pa morata biti v zvezi s tem izpolnjena dva pogoja, in sicer:

1. Pogodbeni obdelovalec mora biti registriran za opravljanje takšne dejavnosti, kar pomeni, da mora biti registriran npr. za obdelavo podatkov (dejavnost pod šifro 72.300 iz Uredbe o uvedbi in uporabi standardne kvalifikacije dejavnosti<sup>24</sup>). V posameznih

---

<sup>24</sup> Uradni list RS, št. 2/2002.

specifičnih primerih, ko se pogodbenemu obdelovalcu poveri npr. samo vodenje računovodstva, obračun plač, izbira kadrov, sklepanje življenjskih zavarovanj, ipd., je dovolj, da je pogodbeni obdelovalec, glede na to, kakšna opravila bo za upravljavca osebnih podatkov opravljal, registriran npr. za računovodske, knjigovodske in revizijske dejavnosti, davčno svetovanje (šifra 74.120), dejavnost posredovanja in zaposlovanja delovne sile (šifra 74.500), življenjsko zavarovanje (šifra 66.010), ipd.

2. Medsebojne pravice in obveznosti morajo biti urejene v pogodbi, ki mora biti obvezno sklenjena v pisni obliki in mora obvezno vsebovati tudi dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov, upravljavec osebnih podatkov pa mora izvajanje dogovorjenih postopkov in ukrepov za zavarovanje osebnih podatkov tudi nadzorovati. V primeru, da pogodba ni sklenjena v pisni obliki ali pa v pogodbi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja niso določeni, kakor tudi če v pogodbi ni določb o nadzoru nad pogodbenim obdelovalcem, bi to pomenilo prekršek po 2. točki prvega odstavka 91. člena ZVOP-1, državni nadzornik za varstvo osebnih podatkov pa lahko v takšnem primeru na podlagi 2. točke prvega odstavka 54. člena ZVOP-1 z odločbo prepove nadaljnjo obdelavo osebnih podatkov. Poleg tega lahko v primeru, ko pogodba nima predpisane oblike, pridejo v poštev tudi določbe 55. člena Obligacijskega zakonika<sup>25</sup>, kjer je določeno, da je pogodba, ki ni sklenjena v predpisani obliki, nična, če iz namena predpisa, s katerim je določena oblika, ne izhaja kaj drugega.

Novost, ki jo v zvezi s pogodbeno obdelavo uvaja ZVOP-1, se dejansko kaže samo v tem, da ZVOP-1 zdaj izrecno določa, kako ravnati v primeru spora med upravljavcem osebnih podatkov in pogodbenim obdelovalcem ter, kako ravnati v primeru prenehanja pogodbenega obdelovalca (npr. stečaja). V praksi je namreč že prišlo do sporov med upravljavcem osebnih podatkov in pogodbenim obdelovalcem, takšnim sporom pa se tudi ne bo mogoče izogniti v bodoče. Zaradi tega je v takšnih primerih edina sprejemljiva rešitev ta, da se zaradi varstva posameznikov, na katere se osebni podatki nanašajo, osebni podatki, ki jih je obdeloval pogodbeni obdelovalec, takoj vrnejo upravljavcu, morebitne kopije pa se takoj uničijo ali pa, če gre v konkretni zadevi za sum kaznivih dejanj, predajo pristojnim državnim organom npr. državnemu tožilstvu, policiji, Urada za preprečevanje pranja denarja Republike Slovenije, sodišču ali Državnemu nadzornemu organu za varstvo osebnih podatkov.

Do primerov, ko upravljavci osebnih podatkov posamezna opravila v zvezi z obdelavo osebnih podatkov poverijo pogodbenim obdelovalcem, v praksi prihaja npr. takrat, ko se zbirke osebnih podatkov vodijo na informacijskem sistemu, ki je last druge pravne ali fizične osebe, ko manjši delodajalci obračun plač ter druge računovodske storitve poverijo računovodskemu servisu, ko operaterji mobilne telefonije ter zavarovalnice za sklepanje naročniških ali zavarovalnih pogodb pooblastijo druge pravne ali fizične osebe, ipd.. Prav tako bi se morale določbe 11. člena ZVOP-1 uporabiti tudi v primeru, ko se vzdrževanje strojne, systemske in aplikativne opreme, ki služi za obdelavo osebnih podatkov, poveri drugi pravni ali fizični osebi ter v primeru, ko se drugo pravno ali fizično osebo pooblasti, da za upravljavca osebnih podatkov izvede takšno zgodovinsko, statistično ali drugo znanstveno raziskavo, za izvedbo katere je potrebno obdelovati tudi zbrane osebne podatke.

Kar zadeva pisne pogodbe s pogodbenim obdelovalcem je potrebno opozoriti, da pogodbe, v katerih je določeno zgolj to, da bo izvajalec vse podatke pridobljene s strani naročnika varoval v skladu z Zakonom o varstvu osebnih podatkov ali v skladu s kakšnim drugim zakonom oziroma

---

<sup>25</sup> Uradni list RS, št. 83/2002.

jih bo varoval kot poslovno skrivnost (kar se v praksi zelo pogosto dogaja), ne ustrezajo določbam 11., 24. in 25. člena ZVOP-1. Glede na določbe prej navedenih členov bi namreč moralo biti v pogodbah jasno določeno, s kakšnimi postopki in ukrepi mora pogodbeni obdelovalec varovati prostore, kjer se nahajajo nosilci osebnih podatkov, s kakšnimi postopki in ukrepi mora varovati sistemsko programsko in aplikativno programsko opremo, s katero se obdelujejo osebni podatki, s kakšnimi postopki in ukrepi se preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih omrežjih, s kakšnimi postopki in ukrepi se zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov ter s kakšnimi postopki in ukrepi se omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil.

V primeru, da ima bodisi upravljavec osebnih podatkov bodisi pogodbeni obdelovalec v svojem notranjem aktu že predpisane ustrezne organizacijske, tehnične in logično tehnične postopke in ukrepe za zavarovanje osebnih podatkov, se lahko namesto tega, da bi se v pogodbi s pogodbenim obdelovalcem te postopke in ukrepe še enkrat jasno določilo, v pogodbi zgolj citira takšen akt, in navede, da je ta akt sestavni del te pogodbe ter, da mora pogodbeni obdelovalec zagotoviti zavarovanje osebnih podatkov v skladu z določbami takšnega akta, ki se ga mora v tem primeru seveda tudi priložiti k pogodbi. V takšnem primeru je potrebno seveda tudi poskrbeti, da se s takšnim aktom seznanijo vsi tisti zaposleni pri upravljavcu osebnih podatkov ter pri pogodbenemu obdelovalcu, ki odgovarjajo za izvajanje dogovorjenih postopkov in ukrepov ter tiste osebe, ki zaradi narave njihovega dela pri upravljavcu osebnih podatkov in pri pogodbenem obdelovalcu obdelujejo določene osebne podatke.

Poleg določitve postopkov in ukrepov za zavarovanje osebnih podatkov bo moralo biti v pogodbi ali aneksu k pogodbi določeno tudi to, na kakšen način bo upravljavec osebnih podatkov pri pogodbenem obdelovalcu nadzoroval izvajanje dogovorjenih postopkov in ukrepov za zavarovanje osebnih podatkov ter katere osebe, ki so zaposlene pri upravljavcu osebnih podatkov, bodo opravljale takšen nadzor. V pogodbi ali aneksu bo moralo biti določeno tudi to, katere osebe, ki so zaposlene pri upravljavcu osebnih podatkov in pri pogodbenem obdelovalcu, lahko zaradi narave njihovega dela opravljajo posamezna opravila v zvezi z obdelavo osebnih podatkov ter kakšna so njihova pooblastila v zvezi s tem in njihove dolžnosti varovanja zaupnosti podatkov. Določeno pa mora biti tudi to, da je posredovanje tako pridobljenih osebnih podatkov naprej mogoče samo z dovoljenjem upravljavca osebnih podatkov.

#### ***5.4. Nepravilnosti in vprašanja, ki se pojavljajo v zvezi s posredovanjem osebnim podatkom drugim uporabnikom ter javnosti***

Ugotovitve kažejo, da se v praksi največ vprašanj pojavlja ravno v zvezi s posredovanjem osebnih podatkov drugim pravnim ali fizičnim osebam. Razlog za pojavljanje takšnih vprašanj leži v dejstvu, da precej uporabnikov osebnih podatkov ne pozna zakonskih podlag, ki bi jih pooblaščale za pridobivanje določenih osebnih podatkov iz zbirk osebnih podatkov, ali pa si uporabniki želijo pridobiti tudi tiste osebne podatke, za katere niso pooblaščeni. Poleg tega se vprašanja v zvezi s posredovanjem oziroma pridobivanjem osebnih podatkov iz zbirk podatkov pojavljajo tudi zaradi nejasnih določb področnih zakonov v zvezi s tem. Zaradi prej navedenih razlogov se upravljavci osebnih podatkov vsakodnevno obračajo na Inšpektorat za varstvo osebnih podatkov ter prosijo za pojasnila in mnenja glede dopustnosti oziroma zakonitosti

posredovanja osebnih podatkov v posameznih konkretnih primerih.

Glede na to, da se v praksi največ vprašanj in zaprosil za mnenja pa tudi največ prijav pojavlja ravno v zvezi s posredovanjem osebnih podatkov drugim uporabnikom ter javnosti, je Inšpektorat za varstvo osebnih podatkov v svojih poročilih o delu za leto 2002 in 2003 že navajal podrobnejša pojasnila v zvezi s to problematiko. Kljub takšnim pojasnilom se število zaprosil za mnenja in tolmačenja v zvezi s posredovanjem osebnih podatkov drugim uporabnikom ter javnosti še naprej povečuje, povečuje pa se tudi število prijav v zvezi s tem. V obravnavanem obdobju je namreč Inšpektorat za varstvo osebnih podatkov prejel skupaj kar 12 prijav zaradi suma nezakonitega posredovanja osebnih podatkov drugim uporabnikom ter javnosti, ki pa so se v večini primerov izkazale za neutemeljene. Kljub temu pa je potrebno opozoriti, da v praksi še vedno prepogosto prihaja do nezakonitega posredovanja osebnih podatkov drugim pravnim oziroma fizičnim osebam. Poglavitni vzroki za takšno nezakonito posredovanje osebnih podatkov so po naših ugotovitvah predvsem malomarnost, nepoznavanje določb Zakona o varstvu osebnih podatkov, želja po pridobitvi materialne ali druge koristi ter želja po maščevanju posamezniku, na katerega se osebni podatki nanašajo.

Ko govorimo o posredovanju osebnih podatkov drugim pravnim oziroma fizičnim osebam je potrebno opozoriti tudi na to, da upravljavci osebnih podatkov posredovanja osebnih podatkov drugim osebam pogosto sploh ne evidentirajo, ali pa je takšno evidentiranje pomanjkljivo. Dolžnost evidentiranja posredovanja osebnih podatkov je upravljavcem osebnih podatkov v letu 2004 nalagal peti odstavek 11. člena ZVOP, po 1. januarju 2005 pa bodo morali upravljavci osebnih podatkov takšno posredovanje evidentirati skladno z določbami tretjega odstavka 22. člena ZVOP-1.

Zadeve, ki se nanašajo na posredovanje osebnih podatkov javnosti, so v obravnavanem obdobju pritegnile tudi daleč največ pozornosti. Gre za sledeče tri zadeve:

- neobvezno mnenje inšpektorja, da policija javnosti ne sme posredovati začetnic imen oseb, ki jih obravnava, saj za takšno sporočanje oziroma posredovanje osebnih podatkov nima zakonske podlage, oziroma je takšno sporočanje osebnih podatkov v nasprotju z določbami ZVOP;
- neobvezno mnenje inšpektorja, da sodišča nimajo zakonske podlage, ki bi jih pooblaščala, da v razporedu obravnav ter sej na oglasni deski javno objavijo tudi osebna imena strank v postopkih;
- odločba inšpektorata, s katero je bilo Banki Slovenije naloženo, da prek svoje spletne strani onemogoči dostop do podatkov o transakcijskih računih o tistih fizičnih osebah, ki niso zasebniki, in sicer vse do takrat, dokler banka za te osebe ne bo zagotovila, da bo mogoče za vsako takšno posredovanje podatkov pozneje ugotoviti, kateri osebi so se v določenem obdobju posredovali podatki iz registra transakcijskih računov o tistih fizičnih osebah, ki niso zasebniki.

Polemika v zvezi z vprašanjem dopustnosti oziroma nedopustnosti posredovanja začetnic imen oseb, ki jih obravnava policija, javnosti, se je pričela, ko je policija na podlagi ustnega mnenja inšpektorja za varstvo osebnih podatkov javnosti prenehala posredovati začetnice imen oseb, ki jih obravnava. Svoje mnenje v zvezi s tem je inšpektor podal na strokovnem posvetu delavcev policije, ki skrbijo za stike z javnostjo. Na tem posvetu, ki je potekal v decembru 2003, so delavci policije inšpektorja seznanili z vsebino njihovega poročanja medijem in njihovimi zagatami pri iskanju ravnovesja med pravico do obveščenosti in pravico do zasebnosti.

Inšpektor je predstavnikom policije povedal, da mora policija pri svojem poročanju upoštevati določbe ZVOP, kar pomeni, da bi lahko javnosti posredovala identifikacijske podatke oseb, ki jih obravnava, le v primeru, če bi bilo tako določeno v nekem zakonu (npr. Zakonu o policiji, Zakonu o medijih, Zakonu o kazenskem postopku, ipd.). Glede na to, da takšnega zakonskega določila ni, je inšpektor predstavnikom policije priporočil, naj v bodoče spremenijo način obveščanja javnosti in sicer tako, da iz njihovih sporočil ne bo več mogoče identificirati oseb, na katere se informacije nanašajo. Po inšpektorjevem mnenju je zaradi preventivnega obveščanja javnosti namreč dovolj, da se javnost seznanj le z dogodkom, krajem ter starostjo oseb, ki so udeležene v posameznem dogodku.

Inšpektor je predstavnikom policije pojasnil, da iz definicije izraza "določljiva oseba" izhaja, da lahko govorimo o obdelavi osebnih podatkov tudi v primeru, če policija ob obravnavi dogodka v nekem manjšem kraju javnosti sporoči zgolj začetnice imen udeležencev, v posameznih primerih pa so posamezniki lahko določljivi oziroma prepoznavni že zgolj na podlagi podatka o njihovi funkciji ali zaposlitvi. Zaradi tega je potrebno zlasti v predkazenskem postopku o dogodkih vedno poročati z vidika domneve nedolžnosti ter ob tem paziti, da se ne škodi časti in dobremu imenu oseb, na katere se informacije nanašajo. Pri nas se namreč žal vse prevečkrat dogaja, da javnost posameznika obsodi že zgolj na podlagi suma, ali pa, da so osebe, zoper katere so bile vložene kazenske ovadbe, z vloženimi ovadbami najprej seznanjene preko medijev.

Mnenje, ki ga je inšpektor ustno predstavil delavcem policije, ki skrbijo za stike z javnostjo, je temeljilo na določbah 15., 35., 38. in 39. člena Ustave RS, določbah 2., 3., 9. in 11. člena ZVOP, določbah 45. člena Zakona o medijih<sup>26</sup> ter določbah 6. člena Zakona o dostopu do informacij javnega značaja<sup>27</sup>.

Po mnenju inšpektorja je bila v obravnavanem primeru ustavna pravica do svobode izražanja in pravica do obveščanosti iz 39. člena Ustave RS omejena s pravicami posameznikov do zasebnosti (35. člen Ustave RS) ter pravico do varstva osebnih podatkov (38. člen Ustave RS). Pri tem po mnenju inšpektorja Ustava RS že sama v svojem 39. členu omejuje pravico do pridobivanja informacij javnega značaja, saj drugi odstavek določa, da ima vsakdo pravico dobiti informacijo javnega značaja, **za katero ima v zakonu utemeljen pravni interes, razen v primerih, ki jih določa zakon.**

Ustavna pravica do pridobivanja informacij se konkretizira v Zakonu o dostopu do informacij javnega značaja ter v 45. členu Zakona o medijih.

Zakon o dostopu do informacij javnega značaja omogoča dostop do vseh informacij, ki izvirajo iz delovnega področja organa, razen do tistih, ki so v 6. členu zakona določene kot izjeme. Tako med drugim organ zavrne dostop do zahtevane informacije tudi v primeru, če se zahteva nanaša na osebni podatek, katerega razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov (3. točka 6. člena ZDIJZ). V primeru izjeme iz 3. točke 6. člena ZDIJZ gre po mnenju inšpektorata za absolutno izjemo, ki organu ali Pooblaščenцу za dostop do informacij javnega značaja ne dopušča nobenega tehtanja med posameznimi pravicami.

Podobno je bilo tudi v 45. členu Zakona o medijih določeno, da javne osebe med drugim

---

<sup>26</sup> Uradni list RS, št. 35/01 in 62/03.

<sup>27</sup> Uradni list RS, št. 24/03.

lahko odrečejo dajanje informacij, če bi to pomenilo kršitev tajnosti osebnih podatkov v skladu z zakonom, razen če se z njihovo objavo lahko prepreči hujše kaznivo dejanje ali neposredna nevarnost za življenje ljudi in njihovo premoženje.

Osebnih podatki so se po določbah 3. člena ZVOP lahko obdelovali le, če je bila obdelava osebnih podatkov določena z zakonom, če je imel upravljavec zbirke osebnih podatkov pisno privolitvev posameznika ter, če je šlo za obdelavo osebnih podatkov oseb, s katerimi je upravljavec zbirke osebnih podatkov v pogodbenem razmerju in je bila obdelava potrebna za izpolnjevanje pogodbenih obveznosti in uveljavljanje pravic iz pogodbenega razmerja. V 9. členu ZVOP je bilo nadalje tudi določeno, da se osebni podatki smejo obdelovati samo za namene določene z zakonom ali s pisno privolitvijo posameznika in ne smejo biti uporabljeni na način, ki ni združljiv s temi nameni.

Iz zgoraj citiranih določb ZVOP ter določb 38. člena Ustave RS je bilo mogoče zaključiti, da je na področju obdelave osebnih podatkov prepovedano vse, kar ni izrecno dovoljeno. Vsako zbiranje in obdelovanje osebnih podatkov namreč predstavlja poseg v ustavno pravico do varstva osebnih podatkov. Poseg je ob upoštevanju načela sorazmernosti dopusten samo v primeru, če je v zakonu določno opredeljeno, kateri osebni podatki se smejo zbirati in obdelovati ter za kakšen namen jih je dovoljeno uporabljati.

Po določbah 3. in 11. člena ZVOP so se lahko osebni podatki sporočali in posredovali le tistim pravnim ali fizičnim osebam, ki so bile za pridobivanje posameznih osebnih podatkov pooblaščen z zakonom ali pa s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo. Če pustimo ob strani pisno privolitvev posameznika, potem je lahko upravljavec zbirke osebnih podatkov (npr. policija) skladno z določbami 3. in 11. člena ZVOP posredoval osebne podatke javnosti samo v primeru, ko je bilo to izrecno določeno v zakonu, ki ureja posamezno področje. To pomeni, da bi moral področni zakon (npr. Zakon o medijih, Zakon o policiji, Zakon o kazenskem postopku, ...) izrecno določiti, da se določeni osebni podatki, ki jih pri opravljanju svojih nalog pridobi policija, lahko posredujejo javnosti. Glede na to, da takšne zakonske določbe ni, lahko policija sporoča javnosti podatke le v obliki in na način, ki ne omogoča identifikacije posameznikov, na katere se informacije nanašajo. Izjema od navedenega je na podlagi 45. člena Zakona o medijih dopustna le v primerih, če se z objavo podatkov lahko prepreči hujše kaznivo dejanje ali neposredna nevarnost za življenje ljudi in njihovo premoženje.

Glede na to, da je Republika Slovenija članica Sveta Evrope, velja na tem mestu opozoriti tudi na Priporočilo št. R(87)15 Komiteja ministrov sveta Evrope državam članicam o ureditvi uporabe osebnih podatkov v policijskem sektorju (Recommendation No. R(87)15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector). Citirano priporočilo je glede uporabe in sporočanja podatkov, zbranih za namene policije izredno restriktivno, saj določa, da se smejo takšni osebni podatki uporabljati izključno za namene opravljanja nalog policije, drugim subjektom pa se smejo posredovati samo v primeru, če za to obstaja jasna zakonska obveznost ali jasno zakonsko pooblastilo ali pooblastilo nadzornega telesa, če je posredovanje podatkov nedvoumno v interesu posameznika, ali, če je posredovanje nujno za preprečitev resne in neposredne nevarnosti.

Inšpektorat za varstvo osebnih podatkov ni pristojen, da bi v posameznih primerih tehtal med pravico do zasebnosti in pravico do varstva osebnih podatkov na eni, ter pravico do obveščenosti na drugi strani, ampak mora presojeti zakonitost obdelave osebnih podatkov (kamor spada tudi sporočanje in uporaba osebnih podatkov) predvsem z vidika določb

ZVOP. Glede na to, da zaenkrat ni zakonske podlage, ki bi javnost pooblašчала pridobivati in uporabljati osebne podatke, ki jih pri svojem delu zbere policija, lahko z vidika določb ZVOP zaključimo, da lahko policija razen v izjemnih primerih obvešča javnost le na način, ki ne omogoča identifikacije posameznikov, na katere se podatki nanašajo.

Če stroka meni, da je javnost upravičena, da se seznanijo z določenimi osebnimi podatki, ki jih pri svojem delu zbere policija, je z vidika določil ZVOP ter določb 35. in 38. člena Ustave RS potrebno v zvezi s tem pripraviti in sprejeti jasne zakonske določbe, ki bodo upoštevale tako interes javnosti, da se seznanijo z določenimi osebnimi podatki, kot tudi pravico do zasebnosti in varstva osebnih podatkov. Ob tem je potrebno poudariti, da Ustava RS in ZVOP sedaj enako ščitita zasebnost in osebne podatke vseh oseb, ne glede na njihov položaj v družbi. To pomeni, da so enako zaščiteni podatki in zasebnost "običajnih" državljanov, funkcionarjev in drugih javnih oseb ter tudi osebni podatki osumljencev, obtožencev in obsojencev.

Da bi javnosti vendarle omogočili, da se v posameznih primerih seznanijo z določenimi osebnimi podatki, ki jih pri svojem delu zbere policija, so predstavniki Inšpektorata za varstvo osebnih podatkov, predstavniki Ministrstva za pravosodje ter predstavniki Policije predlagali dopolnitev 45. člena Zakona o medijih, in sicer na ta način, da se v navedenem členu z vidika načela sorazmernosti jasno določi, v katerih primerih se določeni osebni podatki lahko posredujejo javnosti. Vendar pa takšen predlog kasneje ni bil sprejet, zaradi česar stanje v zvezi s posredovanjem podatkov oseb, ki jih pri svojem delu zbere policija javnosti, ostaja enako, kot je bilo v času, ko je inšpektor predstavnikom policije pojasnil svoje mnenje v zvezi s tem.

Podobno kot je bilo glede posredovanja podatkov s strani policije javnosti, je bilo tudi v primeru neobveznega mnenja inšpektorja, da sodišča nimajo zakonske podlage, ki bi sodišča pooblaščala, da v svojih razporedih obravnav ter se na oglasni deski javno objavijo tudi osebna imena strank v sodnih postopkih. Zakon o sodiščih, ki je veljal v času, ko je inšpektor podal svoje mnenje, namreč ni določal takšne objave.

Po podaji mnenja v zvezi z nedopustnostjo objave osebnih imen strank v sodnih postopkih, je Ministrstvo za pravosodje pripravilo predlog Zakona o spremembah in dopolnitvah Zakona o sodiščih, ki ga je Državni zbor Republike Slovenije sprejel dne 17. junija 2004. V navedenem zakonu<sup>28</sup> je bil med drugim dodan 17a. člen, v katerem je bilo določeno, da razpored obravnav ter se, o katerih se obveščajo stranke in pri katerih javnost po zakonu ali odločitvi sodišča ni izključena, obsega med drugim tudi osebno ime stranke v postopku. Razpored obravnav ter se, o katerih se obveščajo stranke in pri katerih javnost po zakonu ali odločitvi sodišča ni izključena, se skladno z določbami 17a. člena Zakona o sodiščih objavi na oglasni deski sodišča (sodna deska). Sodna deska je deska primerne velikosti, pritrjena na steno sodišča, ki je dostopna javnosti. Podatki na njej se lahko objavijo tudi v elektronski obliki na način, ki zagotavlja dostop javnosti.

Z zgoraj navedenimi spremembami in dopolnitvami Zakona o sodiščih so sodišča pridobila neposredno zakonsko podlago za posredovanje osebnih imen strank v sodnih postopkih javnosti, pri čemer pa moramo opozoriti, da se lahko takšni podatki glede na določbo 17a. člena Zakona o sodiščih posredujejo javnosti le v tistih zadevah, v katerih javnost po zakonu ali odločitvi sodišča ni izključena. Zaradi tega bodo morala sodišča paziti, da po pomoti ali kako drugače ne bo prišlo do objave osebnih imen strank v tistih postopkih, ko je javnost

---

<sup>28</sup> Zakon o spremembah in dopolnitvah Zakona o sodiščih (Uradni list RS, št. 73/2004).

izključena, kar naj bi se po navedbah novinarjev tudi že zgodilo.

Kot že rečeno, je v obravnavanem obdobju veliko pozornosti vzbudila tudi odločba Inšpektorata za varstvo osebnih podatkov, s katero je bilo Banki Slovenije naloženo, da prek svoje spletne strani onemogoči dostop do podatkov o transakcijskih računih o tistih fizičnih osebah, ki niso zasebniki, in sicer vse do takrat, dokler banka za te osebe ne bo zagotovila, da bo mogoče za vsako takšno posredovanje podatkov pozneje ugotoviti, kateri osebi so se v določenem obdobju posredovali podatki iz registra transakcijskih računov o tistih fizičnih osebah, ki niso zasebniki.

Postopek inšpekcijskega nadzora zoper Banko Slovenije se je po uradni dolžnosti pričel iz razloga, ker je Banka Slovenije dne 01.10.2004 na podlagi določb 20. člena Zakona o spremembah in dopolnitvah zakona o plačilnem prometu<sup>29</sup> omogočila tudi iskanje podatkov o transakcijskih računih tistih fizičnih oseb, ki niso zasebniki. S prej navedeno določbo Zakona o plačilnem prometu, ki se je pričela uporabljati 01.10.2004, so se spremenile določbe prej veljavnega 29. člena Zakona o plačilnem prometu in sicer tako, da je zakon sedaj določal, da so podatki o transakcijskih računih javni in dostopni na spletni strani Banke Slovenije.

Pred uveljavitvijo zgoraj navedene novele Zakona o plačilnem prometu je bilo v 29. členu določeno, da podatke o transakcijskih računih imetnikov transakcijskih računov, ki so druge fizične osebe, lahko zahteva samo:

- imetnik transakcijskega računa glede podatkov, ki se nanašajo nanj;
- sodišče oziroma drug pristojni državni organ, če jih potrebuje v postopku, ki ga vodi v okviru svojih pristojnosti.

Banka Slovenije je po uveljavitvi zgoraj navedene novele prek svojih spletnih strani omogočila iskanje podatkov, ki so se nanašali na fizične osebe na več načinov, in sicer:

- z vnosom št. transakcijskega računa;
- z vnosom imena in priimka fizične osebe;
- z vnosom imena in priimka ter davčne številke ter
- z vnosom imena in priimka ter ulice (brez hišne številke) in kraja.

Sistem pred vnosom podatkov v iskalnik oziroma pred iskanjem podatkov od osebe, ki išče podatke, ni zahteval vnosa podatkov, iz katerih bi bilo razvidno, katera oseba poizveduje za podatki določene oziroma določljive fizične osebe. Sistem tudi ni omogočal možnosti poznejšega ugotavljanja, kateri osebi so bili posredovani podatki o transakcijskem računu določenega posameznika prek spletnih strani Banke Slovenije.

V primeru iskanja podatkov o fizičnih osebah, ki niso zasebniki, prek spletnih strani na enega od zgoraj opisanih načinov, se je posamezniku, ki je prek spletnih strani iskal podatke, odprlo okno, iz katerega so bili razvidni sledeči podatki, ki so se nanašali na fizično osebo, ki ni zasebnik: št. transakcijskega računa, oznaka za IBAN, vrsta računa, evidenca o neporavnanih obveznostih, status računa, ime banke, ki vodi transakcijski račun, ime in priimek imetnika transakcijskega računa, kraj stalnega bivališča imetnika računa (pošta) ter datum odprtja, zadnje spremembe in zaprtja transakcijskega računa.

Po mnenju inšpektorata zgoraj opisani način posredovanja podatkov o imetnikih transakcijskih računov ni zadostil zahtevam iz petega odstavka 11. člena ZVOP, po katerem je moral

---

<sup>29</sup> Uradni list RS, št. 37/2004.



zavezanec kot upravljavec zbirke osebnih podatkov za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani ter predvsem komu so bili posredovani osebni podatki določenega imetnika transakcijskega računa. Takšen sistem zaradi tega tudi ni omogočil uresničitve pravice posameznika iz 18. člena ZVOP, kateremu je bil zavezanec dolžan posredovati seznam subjektov, katerim so bili v določenem obdobju posredovani njegovi osebni podatki.

Opisan način posredovanja osebnih podatkov po mnenju inšpektorata tudi ni zagotavljal ustreznega zavarovanja osebnih podatkov v skladu z določbami 13. in 14. člena ZVOP-a, saj ni zagotavljal možnosti naknadnega ugotavljanja, kdo je uporabil osebne podatke določenega imetnika transakcijskega računa, ki je druga fizična oseba.

Pooblaščenec Banke Slovenije je v postopku pojasnil, da »Zakon o plačilnem prometu, ki je bil sprejet kasneje kot Zakon o varstvu osebnih podatkov, v 29. členu določa javnost podatkov za vse imetnike transakcijskih računov in dostopnost do teh podatkov prek spletnih strani Banke Slovenije. Glede na določbo o dostopnosti prek spletne strani, izhaja, da ni potrebno zagotoviti sledljivosti podatkov kot to zahteva Zakon o varstvu osebnih podatkov. Takšen tudi ni bil namen zakonodajalca, ki je z določbo o dostopnosti na spletni strani želel doseči poenostavljen dostop do teh podatkov. Določbe 29. člena Zakona o plačilnem prometu derogirajo določbe 11. in 18. člena Zakona o varstvu osebnih podatkov o sledljivosti dostopa do teh podatkov. Tudi določbe petega odstavka 11. ZVOP-a zahtevajo sledljivost podatkov samo za točno določen namen in sicer varovanja in kontrole nedopustnega posredovanja osebnih podatkov. Podatki, ki so v skladu z že omenjenimi določbami Zakona o plačilnem prometu javni in dostopni na spletni strani Banke Slovenije, ne morejo biti nedopustno posredovani, saj za njihovo posredovanje vsem zainteresiranim obstaja nedvoumna zakonska podlaga.«

Inšpektorat se s takšnim pojasnilom ni strinjal in je odločil, da je v postopku ugotovljeno dejansko stanje v nasprotju z določbami petega odstavka 11. člena ZVOP, ki določa, da mora upravljavec zbirke osebnih podatkov, to je zavezanec, za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani ter komu in na kakšni podlagi so bili podatki posredovani in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov. Ugotovljeno dejansko stanje je sicer omogočalo možnost naknadnega ugotavljanja, kateri osebni podatki so bili posredovani ter na kakšni pravni podlagi so bili podatki posredovani, vendar pa takšen sistem nedvoumno ni omogočal možnosti poznejšega ugotavljanja, **kateri osebi** so bili osebni podatki posameznika posredovani. Takšno evidentiranje posredovanja je bilo potrebno zaradi določb 3. točke prvega odstavka 18. člena ZVOP, ki določa pravice posameznika oziroma upravljavca zbirke osebnih podatkov zavezuje, da posamezniku, na katerega se podatki nanašajo, na njegovo zahtevo posreduje seznam subjektov, katerim so bili v določenem obdobju posredovani osebni podatki, ki so vsebovani v zbirki in se nanašajo nanj.

Zgoraj navedeno pravico posameznika je po mnenju inšpektorata mogoče skladno z določbami 23. člena ZVOP-a omejiti samo za zakonom, pri čemer pa veljavni Zakon o plačilnem prometu ni določal takšne omejitve pravic posameznika. V 29. členu Zakona o plačilnem prometu je bilo dejansko določeno le to, da so podatki o transakcijskih računih javnih in dostopni na spletni Strani Banke Slovenije, pri čemer pa prej navedeni zakon nikjer ne določa, da Banki Slovenije ni potrebno evidentirati vpogleda v osebne podatke, kot je to določeno npr. v četrtem odstavku 77. člena Zakona o evidentiranju nepremičnin, državne meje in prostorskih enot<sup>30</sup>.

---

<sup>30</sup> Uradni list RS, št. 52/2000.

Prav tako Zakon o plačilnem prometu nikjer ne omejuje zgoraj navedene pravice posameznika iz 18. člena ZVOP-a, ki se lahko, kot že rečeno, skladno z določbami 23. člena ZVOP omeji samo z zakonom. Zaradi tega se ne more upoštevati zgoraj navedenih pripomb zavezanca, da zavezancu glede na določbo o dostopnosti do podatkov prek spletne strani ni potrebno zagotoviti sledljivosti podatkov, kot to zahteva ZVOP. Določbo 29. člena Zakona o plačilnem prometu glede javnosti podatkov ter dostopa do podatkov prek spletnih strani je bilo z vidika določb 11. člena ZVOP možno šteti le kot zakonsko podlago, ki vsakogar pooblašča, da si pridobi podatke o transakcijskem računu katere koli fizične osebe.

Navedbo zavezanca, da določbe 29. člena Zakona o plačilnem prometu derogirajo določbe 11. in 18. člena ZVOP ter, da je Zakon o plačilnem prometu poznejši zakon kot ZVOP, torej po mnenju inšpektorata ni bilo mogoče upoštevati, saj Zakon o plačilnem prometu v nobenem od svojih členov ne derogira določb 11. in 18. člena systemskega zakona, to je ZVOP. Ker Zakon o plačilnem prometu nikjer ne derogira določb 11. in 18. člena ZVOP to pomeni, da se v zvezi z evidentiranje posredovanja osebnih podatkov drugim uporabnikom subsidiarno uporabljajo določbe systemskega zakona, saj se namen systemskega zakona kaže ravno v tem, da se z njim zapolnijo pravne praznin v področnih zakonih.

Banka Slovenije se je na odločbo Inšpektorata za varstvo osebnih podatkov pritožila, ministrica za pravosodje pa je kot organ druge stopnje zaradi napačne uporabe materialnega predpisa odpravila odločbo inšpektorja in hkrati sama odločila o stvari. Odločila je tako, da je Banki Slovenije odredila, da takoj po vročitvi njene odločbe onemogoči dostop prek svoje spletne strani do podatkov o transakcijskih računih tistih fizičnih oseb, ki niso zasebniki.

V zgoraj opisanem primeru gre po mnenju inšpektorata za tipičen primer področnega zakona (Zakon o plačilnem prometu), ki z določbo »Podatki o transakcijskih računih so javni in dostopni na spletni strani Banke Slovenije« prekomerno posega v pravice imetnikov transakcijskih računov do varstva njihovih osebnih podatkov. Po mnenju inšpektorata je namreč zakonodajalec pred sprejemom takšne določbe premalo pretehtal dopustnost takšnega posega v ustavno pravico do varstva osebnih podatkov, pri čemer pa Inšpektorat za varstvo osebnih podatkov ne more odločati o tem, ali posamezne določbe področnega zakona morebiti preveč posegajo v to pravico, saj lahko o tem odloča le Ustavno Sodišče Republike Slovenije.

Da bi se v bodoče izognili zakonskim določbam, ki preveč posegajo v pravico posameznika do varstva osebnih podatkov, je zakonodajalec z novim Zakonom o varstvu osebnih podatkov (ZVOP-1) Državni nadzorni organ za varstvo osebnih podatkov pooblastil za dajanje predhodnih mnenj ministrstvu, Državnemu zboru, organom samoupravnih lokalnih skupnosti ter drugim organom o usklajenosti določb predlogov zakonov ter ostalih predpisov za zakoni in drugimi predpisi, ki urejajo osebne podatke. Poleg tega bo lahko Državni nadzorni organ na podlogi 48. člena ZVOP-1 od 1. januarja 2006 dalje na Ustavno sodišče Republike Slovenije vložil tudi zahtevo za oceno ustavnosti zakonov, ostalih predpisov ter splošnih aktov, izdanih za izvrševanje javnih pooblastil, če bo nastalo vprašanje ustavnosti in zakonitosti v zvezi s postopkom, ki ga bo vodil.

### **5.5. Obdelava prekomernih in nepotrebnih osebnih podatkov**

Javni sektor (državni organi, organi samoupravnih lokalnih skupnosti, nosilci javnih pooblastil, javne agencije, javni skladi, javni zavodi, univerze, samostojni visokošolski zavodi

in samoupravne narodne skupnosti) lahko primarno obdelujejo le tiste osebne podatke, za katere je to določeno z zakonom. Navedeno pomeni, da je dejansko predlagatelj in kasneje zakonodajalec tisti, ki določa, katere osebne podatke lahko posamezni obdelovalci osebnih podatkov na področju javnega sektorja sploh obdelujejo. To hkrati tudi pomeni, da morata predlagatelj zakona in zakonodajalec v fazi sprejemanja zakona pretehtati, katere vrste osebnih podatkov so dejansko potrebne za opravljanje posamezne naloge oziroma pooblastila, ki je zaupano upravljavcu osebnih podatkov na področju javnega sektorja, oziroma morata paziti, da bodo osebni podatki, ki se bodo obdelovali, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo (načelo sorazmernosti).

Za razliko od javnega sektorja lahko zasebni sektor poleg osebnih podatkov, ki jih za posamezne primere določa zakona, obdeluje osebne podatke tudi na podlagi osebne privolitve posameznika. Takšna zakonska ureditev v praksi pogosto pripelje do izsiljevanja posameznika in prekomernega zbiranja osebnih podatkov na področju zasebnega sektorja, pri čemer pa inšpektor v obravnavanem obdobju niti ni mogel ustrezno ukrepati, saj ZVOP zasebnemu sektorju dopušča obdelavo osebnih podatkov tudi na podlagi pisne privolitve posameznika. Inšpektor torej v obravnavanem obdobju ni imel pravne podlage, na podlagi katere bi lahko presojal, ali gre v konkretni zadevi za obdelavo prekomernih osebnih podatkov oziroma katere vrste osebnih podatkov so odveč glede na namene, zaradi katerih se obdelujejo. Po našem mnenju bo to pravno praznino z opredelitvijo načela sorazmernosti do neke mere odpravil ZVOP-1.

Kar zadeva obdelavo osebnih podatkov na podlagi osebne privolitve posameznika je treba opozoriti, da upravljavci osebnih podatkov v praksi pred zbiranjem osebnih podatkov posameznike pogosto pomanjkljivo seznanijo z osebnimi podatki. Najpogostejša razloga za takšno pomanjkljivo seznanitev sta predvsem slabo poznavanje določb Zakona o varstvu osebnih podatkov ali pa poizkus zavajanja posameznikov glede nadaljnje obdelave osebnih podatkov. Tudi v zvezi s tem problemom v prihodnjem obdobju pričakujemo izboljšanje, saj novi ZVOP-1 zdaj v svojem 19. členu natančneje določa informacije, ki jih je potrebno posredovati posamezniku ob zbiranju njegovih osebnih podatkov.

Kot kažejo ugotovitve, zasebna podjetja tudi pred sklepanjem raznih pogodb od posameznika pogosto zahtevajo, da jim le ta posreduje celo vrsto svojih osebnih podatkov, med katerimi so pogosto tudi takšni, ki za sklenitev ali izvajanje posamezne pogodbe ali za opravljanje določne dejavnosti sploh niso potrebni. Največ primerov prekomernega zbiranja osebnih podatkov se pojavlja pri sklepanju delovnih razmerij, dajanju kreditov, izdajanju raznih plačilnih kartic ter pri sklepanju raznih naročniških razmerij. Takšnemu prekomernemu zbiranju osebnih podatkov se je lahko posameznik uprl le na ta način, da je odkloni posredovanje določenih osebnih podatkov oziroma oddal nepopolno vlogo, posledica takšne odklonitve pa se je lahko pokazala v tem, da je ponudnik zavrnil vlogo posameznika in si je moral posameznik zaradi tega poiskati novega ponudnika ali pa dopolniti svojo vlogo in navesti vse zahtevane osebne podatke. V obravnavanem obdobju inšpektor za varstvo osebnih podatkov v takšnih primerih ni mogel ukrepati, se pa bo stanje verjetno spremenilo s 1. januarjem 2005. ZVOP-1 namreč poleg splošnega načela sorazmernosti (3. člen ZVOP-1), v 9. in 10. členu tudi omejuje obdelavo osebnih podatkov za namene sklepanja pogodb ali za namene izpolnjevanja pogodb, saj iz določb navedenih členov izhaja, da se lahko za te namene osebni podatki obdelujejo le, če je obdelava osebnih podatkov **potrebna in primerna** za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe.

## **5. PRIPOROČILA ZA IZBOLJŠANJE STANJA NA PODROČJU VARSTVA OSEBNIH PODATKOV V REPUBLIKI SLOVENIJI**

Iz v tem poročilu predstavljenih najpogosteje ugotovljenih nepravilnosti je mogoče zaključiti, da je stanje na področju varstva osebnih podatkov v Republiki Sloveniji mogoče izboljšati predvsem z izobraževanjem ter osveščanjem oseb, ki so pri upravljalcih osebnih podatkov odgovorne za obdelavo osebnih podatkov, saj so ravno upravljalci osebnih podatkov tisti, ki lahko največ prispevajo ki izboljšanju stanja na tem področju. S tem namenom so v tem in preteklih poročilih nekatere dileme, ki se vsakodnevno pojavljajo v praksi, že podrobneje pojasnjene.

Možnosti za izboljšanje stanja v smislu preventivnega ukrepanja in osveščanja javnosti se dodatno odpirajo tudi z uveljavitvijo ZVOP-1, s katerim je Inšpektorat za varstvo osebnih podatkov oziroma bodoči Državni nadzorni organ za varstvo osebnih podatkov poleg nadzornega in prekrškovnega organa postal tudi neke vrste svetovalni organ, ki lahko na podlagi 49. člena ZVOP-1 pripravlja in izdaja tudi notranje glasilo in strokovno literaturo s področja varstva osebnih podatkov ter pripravlja, daje in objavlja neobvezna mnenja, navodila in priporočila glede varstva osebnih podatkov na posameznih področjih. Na tej podlagi bo torej lahko inšpektorat oziroma bodoči nadzorni organ v sodelovanju s stroko, upravljalci osebnih podatkov in pristojnimi ministrstvi pripravljati in objavljati priporočila in navodila glede obdelave osebnih podatkov na tistih področjih, na katerih se v praksi pojavlja največ vprašanj in nepravilnosti. Takšna navodila in priporočila bodo za upravljalce osebnih podatkov sicer neobvezna, vendar pa bodo po našem mnenju kljub temu lahko precej prispevala k izboljšanju stanja na posameznem področju.

Nedvomno lahko k izboljšanju stanja na področju varstva osebnih podatkov zelo veliko prispeva tudi okrepitev tako imenovanega preventivnega inšpekcijskega nadzora pri upravljalcih osebnih podatkov, saj se je v preteklosti izkazalo, da imajo področje varstva osebnih podatkov praviloma najboljše urejeno ravno tisti upravljalci osebnih podatkov, pri katerih je bil že opravljen inšpekcijski nadzor nad izvajanjem določb Zakona o varstvu osebnih podatkov.

Zgoraj omenjenih možnosti za izboljšanje stanja se na Inšpektoratu za varstvo osebnih podatkov vseskozi zelo dobro zavedamo. Vendar pa nas pri njihovem uresničevanju ovira predvsem premajhno število zaposlenih na inšpektoratu, saj smo le trije zaposleni nedvomno premalo za uspešno opravljanje vseh nalog in pristojnosti, ki jih inšpektoratu nalaga zakon. Naloge in pristojnosti Inšpektorata za varstvo osebnih podatkov so se s 1. januarjem 2005, ko je stopil v veljavo ZVOP-1, še bistveno povečale glede na do takrat veljavni zakon, zaradi česar bi bilo potrebno za učinkovito opravljanje z zakonom določenih nalog in pristojnosti takoj povečati število inšpektorjev za varstvo osebnih podatkov – bodočih državnih nadzornikov.

Za primerjavo navajajmo število oseb, ki so bile v letu 2004 zaposlene v nadzornih organih za varstvo osebnih podatkov v nekaterih drugih evropskih državah ter število prebivalcev v teh državah (v milijonih)<sup>31</sup>:

<b>Država:</b>	<b>Št. zaposlenih v NO za VOP:</b>	<b>Št. prebivalcev (v milijonih):</b>
Avstrija	20	8
Belgija	10	10,3

<sup>31</sup> Vir: Povzetek vprašalnika s Spomladanske konference evropskih nadzornih organov za varstvo osebnih podatkov; Krakow 25. do 26. april 2005.

Bolgarija	15	8
Češka	79	10
Danska	26	5,3
Estonija	31	1,4
Finska	20	5,2
Francija	83	62
Nemčija	64	82,5
Grčija	83	10
Madžarska	10	10
Islandija	6	0,3
Irska	19	4
Italija	94	58
Latvija	23	2,3
Liechtenstein	1	0,034
Nizozemska	65	16
Norveška	29	4,5
Poljska	115	38,2
Portugalska	15	10,4
Litva	30	3
Slovenija	3	2
Monako	7	0,03
Romunija	37	22
Slovaška	33	5,37
Španija	97	43,2
Švedska	39	9
Švica	20	7
Velika Britanija	205	59,5

Iz zgoraj navedene tabele je razvidno, da je Republika Slovenija glede števila oseb, ki so na milijon prebivalcev zaposlene v nadzornem organu za varstvo osebnih podatkov, na samem repu med evropskimi državami.

Problematike kadrovske podhranjenosti Inšpektorata za varstvo osebnih podatkov smo se na inšpektoratu sicer vseskozi zavedali in ta problem izpostavljali v vseh naših preteklih poročilih ter dopisih pristojnim organom, vendar pa smo bili pri naših poizkusih za kadrovske okrepitve inšpektorata očitno neuspešni.

Možnosti za izboljšanje stanja na področju varstva osebnih podatkov se kažejo tudi v potrebi po večji usklajenosti področne zakonodaje z določbami Zakona o varstvu osebnih podatkov in ostalimi predpisi s področju varstva osebnih podatkov. Usklajenost področne zakonodaje s predpisi s področja varstva osebnih podatkov se je v zadnjih letih sicer bistveno izboljšala, saj so novo sprejeti zakoni ali novele zakonov praviloma že usklajeni z določbami Zakona o varstvu osebnih podatkov, vendar pa to kljub temu ne velja za vse področne zakone. Da bi se stanje izboljšalo, je Vlada Republike Slovenije dne 15.04.1999 in dne 17.05.2001 na podlagi poročila inšpektorja za varstvo osebnih podatkov že sprejela sklepe, s katerimi je ministrstva zadolžila, da v okviru svojega delovnega področja preverijo usklajenost področnih zakonov z določbami ZVOP ter v sodelovanju s pristojno službo Ministrstva za pravosodje pripravijo ustrezne rešitve, vendar pa navedena sklepa v praksi nista v celoti uresničena.

Po našem mnenju bo na področju usklajevanja področne zakonodaje s predpisi s področja varstva osebnih podatkov v bodoče potrebno posveti še precej pozornosti. Pri tem ne mislimo le na usklajevanje materialne zakonodaje, pač pa tudi na usklajevanje procesne zakonodaje (npr. Zakon o splošnem upravnem postopku, Zakon o kazenskem postopku), ki s svojimi določbami glede javne objave sodb (npr. 179. člen Kazenskega zakonika v povezavi s 364. in 227. členom Zakona o kazenskem postopku), javne razglasitve upravnih odločb (peti odstavek 155. člena Zakona o splošnem upravnem postopku) ter pregledovanja spisov (npr. 82. člen Zakona o splošnem upravnem postopku) pogosto prekomerno posegajo v pravico posameznikov do varstva njihove zasebnosti in osebnih podatkov.

Da bi se stanje v zvezi z usklajenostjo področne zakonodaje izboljšalo, predlagamo ustanovitev posebne ekspertne skupine, ki bi opravila analizo usklajenosti področne zakonodaje s predpisi o varstvu osebnih podatkov ter na podlagi te analize pristojnim ministrstvom predlagala ukrepe za odpravo ugotovljenih neskladij. V analizi bi bilo potrebno presoditi, ali posamezni področni zakoni dovolj natančno določajo obdelavo osebnih podatkov (npr. vrste osebnih podatkov, ki se obdelujejo, način zbiranja, čas shranjevanja, namen obdelave osebnih podatkov, morebitne omejitve pravic posameznika) ter ob tem z vidika načela sorazmernosti presoditi, ali so osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.

*Pripravil:*

*Jože BOGATAJ*

*v.d. glavnega inšpektorja za varstvo osebnih podatkov*