UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo
visokošolskega programa

VARSTVO OSEBNIH PODATKOV V POLICIJI

Kandidat: Simon LIKAR
Št. indeksa: 04031871

Mentor: izr. prof. dr. Marjan BREZOVŠEK

Ljubljana, januar 2009

POVZETEK

Varstvo osebnih podatkov doživlja preporod. V sodobnem razvitem, s tehnologijo naphanem svetu, se posamezniki vse bolj zavedamo občutljivosti podatkov in ranljivosti posameznika v sistemu, ki ni podprt s sodobno in učinkovito pravno podlago. Bistvo dobrega sistema je, da posamezniku omogoča pregled in vpogled v obdelavo svojih osebnih podatkov, ob tem pa pri sumu zlorabe tudi možnost pritožbe.
Policija je zagotovo v vseh sistemih organ, ki ima dostop do velike količine osebnih podatkov, od splošnih pa do zelo občutljivih. V diplomski nalogi bom predstavil splošne in posamične pravne akte ter druge ukrepe, ki pripomorejo k temu, da je slovenska policija na področju varstva osebnih podatkov postala moderna evropska policija s transparentnim ravnanjem z osebnimi podatki, visoko ravnijo nadzora ter enostavno možnostjo vpogleda in pritožbe ob sumu kršitev.

KLJUČNE BESEDE:

Osebni podatek, varstvo osebnih podatkov, ZVOP-1, policija, načela, informacijski pooblaščenec, katalog zbirk osebnih podatkov, direktiva EU 95/46/ES.

SUMMARY

Personal data protection is becoming a very topical subject again. In modern, developed and technological world individuals are aware of personal data sensitivity and vulnerability in a system which is not supported by modern and effective legal basis. A good system enables an individual to check the processing of personal data and to complain if there is a suspicion of abuse.
The police is definitely the institution in all systems which has the access to personal data, from general to very sensitive ones. In my diploma I discuss the general and individual legal acts, and other measures which have helped that, in the field of personal data protection, the Slovenian Police has become a modern European Police institution with transparent personal data, a high level supervision, and a simple way of checking and complaining about the suspicion of abuse.

KEY WORDS:

personal data, personal data protection, Personal Data Protection Act, the police, principles, an information commissioner, the catalogue of personal data collection, directive EU 95/46/ES.

KAZALO

1 UVOD 1

1.1 NAMEN IN CILJI NALOGE 2

1.2 STRUKTURA DIPLOMSKEGA DELA 2

2 OPREDELITEV OSNOVNIH POJMOV 3

2.1 ZASEBNOST KOT TEMELJNA ČLOVEKOVA PRAVICA 4

3 ZGODOVINA VARSTVA OSEBNIH PODATKOV 6

3.1 RAZVOJ VARSTVA OSEBNIH PODATKOV 6

3.2 PRVA NACIONALNA ZAKONODAJA NA PODROČJU VARSTVA OSEBNIH PODATKOV . 8

4 NORMATIVNA UREDITEV 9

4.1 KONVENCIJA O VARSTVU POSAMEZNIKOV GLEDE NA AVTOMATSKO OBDELAVO PODATKOV 9

4.1.1 Načela v Konvenciji Evropskega sveta o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov 10

4.2 DIREKTIVA O VARSTVU POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV IN O PROSTEM PRETOKU PODATKOV 12

4.3 USTAVA RS KOT NEPOSREDNA PODLAGA ZA ZAKONSKO UREDITEV VARSTVA OSEBNIH PODATKOV 14

4.4 ZAKON O VARSTVU OSEBNIH PODATKOV (ZVOP-1) 15

4.4.1 Splošne določbe - I. DEL (1.-7. člen) 16
4.4.2 Obdelava osebnih podatkov – II. DEL (8.–28. člen) 17
4.4.3 Pravice posameznika – III. DEL (29. do 36. člen) 19
4.4.4 Institucionalno varstvo osebnih pravic – IV. DEL (37. do 61. člen) 19
4.4.5 Iznos osebnih podatkov – V. DEL (62.–71. člen) 20
4.4.6 Področne ureditve – VI. DEL (72.–90. člen) 20
4.4.7 Kazenske določbe - VII. DEL (91.–103. člen) 20
4.4.8 Prehodne in končne določbe – VIII. DEL (104.–117. člen) 21

4.5 Mnenje o ZVOP-1 21

4.6 ZAKON O DOSTOPU DO INFORMACIJ JAVNEGA ZNAČAJA 21

4.7 KAZENSKI ZAKONIK 23

4.8 Ostali zakoni 23

5 ORGANI VARSTVA OSEBNIH PODATKOV 24

5.1 RAZVOJ DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA 24

5.2 RAZVOJ V SLOVENIJI 24

5.3 INFORMACIJSKI POOBLAŠČENEC 25
5.3.1 Pristojnosti informacijskega pooblaščenca na podlagi ZVOP-1: 26
5.3.2 Pristojnosti informacijskega pooblaščenca na področju dostopa do informacij javnega značaja 29

5.4 VARUH ČLOVEKOVIH PRAVIC 29

6 VARSTVO OSEBNIH PODATKOV V POLICIJI 31

6.1 ZAKON O POLICIJI 31

6.2 PRAVILNIK O VAROVANJU PODATKOV POLICIJE 32

6.3 KATALOG ZBIRK OSEBNIH PODATKOV V POLICIJI 37

6.4 DRUGI PREDPISI 41

6.5 SCHENGENSKI INFORMACIJSKI SISTEM IN VARSTVO PODATKOV 41
6.5.1 Zavarovanje in nadzor nad varstvom osebnih podatkov v SIS 44

7 PRIMERI IZ PRAKSE 45

7.1 NEUPRAVIČENO POSREDOVANJE PODATKOV LOVSKI DRUŽINI 45

7.2 (NE)POSREDOVANJE OSEBNIH PODATKOV PRIJAVITELJA KAZNIVEGA DEJANJA 46

8 ZAKLJUČEK 48

LITERATURA 50

VIRI 50

SPLETNE STRANI 51

PRILOGA 1 53

PRILOGA 2 54

PRILOGA 3 56

9 IZJAVA O AVTORSTVU IN NAVEDBA LEKTORJA 57

1 UVOD

V današnjem svetu, ki je prepleten z modernimi informacijskimi tehnologijami, je vse teže zagotavljati varstvo osebnih podatkov, vse več je posegov v našo zasebnost, ki se jih mnogokrat niti ne zavedamo, ne zavedamo pa se tudi posledic, ki jih ti posegi prinašajo.

Dostop do informacij javnega značaja intenzivneje posega v naš pravni red in nas vznemirja šele v zadnjem času, saj je v Republiki Sloveniji prvi celoviti zakon, ki je obravnaval dostop do informacij javnega značaja, začel veljati šele v začetku leta 2003, kljub temu da je pravica dostopa do informacij javnega značaja urejena že kot ustavna kategorija v Ustavi Republike Slovenije, ki v 39. členu to pravico uvršča v kategorijo človekovih pravic in svoboščin. Po svoji naravi omogoča vpogled v delovanje državnih organov in posledično omogoča nadzor nad delom organov ter odraža bistvo demokracije.

Od leta 1990, ko je Slovenija dobila prvi zakon, ki je urejal varstvo osebnih podatkov, je bilo to področje še dvakrat reformirano. Vsaka sprememba prinaša večjo zahtevnost pri upravljanju s tem področjem in nekatere nove inštitute, ki se z vsako spremembo reformirajo, včasih do te mere, da so dotedanje izkušnje lahko celo obremenilne pri njihovem pravilnem uvajanju v prakso. Vzporedno s spremembami predpisov in posameznih inštitutov se ustanavljajo in reformirajo tudi organi, katerih glavna skrb naj bi bila namenjena zagotavljanju pogojev za ustrezno institucionalno varstvo osebnih podatkov.

Varstvo osebnih podatkov in dostop do informacij javnega značaja sta pravici, ki se pogosto stikata ob navidez tektonski prelomnici javnega in zasebnega. V zadnjem času nasploh silijo v ospredje razmerja med javnim sektorjem in uporabniki storitev. Ne le da ta razmerja zagotavljajo ustrezno prilagajanje javnega sektorja potrebam državljanov, temveč tudi blažijo negativne učinke brezosebnega odnosa med javnim sektorjem in državljani ter povečujejo transparentnost njegovega delovanja. Posameznik je v razmerju do države v nezavidljivem položaju, saj je brez ustreznih informacij o delovanju države, razlogih za obravnavanje njegovih osebnih podatkov, dejansko omejen z možnostmi uspeha in brez ustreznega razumevanja postopkov, ki vplivajo na zadovoljevanje njegovih lastnih interesov.

Področja zdravstva, notranjih zadev, policije, pravosodja, socialnega varstva in druga, so tista, pri katerih je obdelava osebnih podatkov pogosta, obenem pa je interes posameznikov po pridobivanju informacij o njihovem urejanju izjemno velik. Ta področja po svoji naravi predstavljajo stičišče obeh pravic, varstva osebnih podatkov in dostopa do informacij javnega značaja.

1.1 NAMEN IN CILJI NALOGE

V Policiji sem zaposlen že nekaj časa in vsakodnevno se srečujem z uporabo osebnih podatkov v službene namene. Dostopa do podatkov, evidenc in raznih seznamov je res ogromno. Skozi diplomsko nalogo sem zato nanizal vse najpomembnejše pravne akte s tega področja, od zgodovinskih, evropskih, Ustave RS, vseh pomembnejših zakonov in nazadnje pravilnikov, internih usmeritev in katalogov Policije. Namen tega je skozi predstavitev pravne ureditve, ki je po mojem mnenju dobra in sodobna, povsem primerljiva z bolj razvitimi državami, dokazati da deluje tudi v praksi, konkretno v Policiji.

1.2 STRUKTURA DIPLOMSKEGA DELA

Diplomsko delo je razdeljeno na sedem poglavij, vsako od teh pa ima še podpoglavja.
V uvodu je predstavljen namen in cilji naloge ter struktura. Prvo poglavje obdeluje razlago osnovnih pojmov ter opredeli zasebnost kot eno od temeljnih človekovih pravic. Drugo poglavje obdeluje zgodovino varstva osebnih podatkov, tretje, po mojem mnenju najpomembnejše poglavje, pa vse pravne vire, ki so ključni za raven varstva osebnih podatkov, kakršno imamo danes. V četrtem delu so predstavljeni organi varstva osebnih podatkov, Informacijski pooblaščenec in Varuh človekovih pravic. Peto poglavje je poglavje o varstvu osebnih podatkov v Policiji. Predstavljeni so zakonski in podzakonski akti, ki urejajo to področje, Katalog zbirk osebnih podatkov ter varovanje podatkov v okviru Schengenskega informacijskega sistema. Praktična primera kršitve zakonodaje in učinkovitega reševanja pa sta opisana v šestem poglavju. V sedmem sledi še zaključek.

2 OPREDELITEV OSNOVNIH POJMOV

OSEBNI PODATEK – je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.

POSAMEZNIK – je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko posredno ali neposredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

OBDELAVA OSEBNIH PODATKOV – pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov; zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).

AVTOMATIZIRANA OBDELAVA – je obdelava osebnih podatkov s sredstvi informacijske tehnologije.

ZBIRKA OSEBNIH PODATKOV – je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

UPRAVLJALEC OSEBNIH PODATKOV – je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma osebe, določene z zakonom, ki določa tudi namene in sredstva obdelave.

POSREDOVANJE OSEBNIH PODATKOV – je posredovanje ali razkritje osebnih podatkov.

KATALOG ZBIRKE OSEBNIH PODATKOV – je opis zbirke osebnih podatkov.

REGISTER ZBIRK OSEBNIH PODATKOV – je register, v katerem so podatki iz katalogov zbirk osebnih podatkov.

PISNA PRIVOLITEV POSAMEZNIKA – je podpisana privolitev posameznika, ki ima obliko listine, določila v pogodbi, določila v naročilu, priloge k vlogi ali drugo obliko v skladu z zakonom, podpis pa je tudi na podlagi zakona s podpisom izenačena oblika, podana s telekomunikacijskim sredstvom, ki jo poda posameznik, ki ne zna ali ne more drugače pisati.

BLOKIRANJE – je takšna označitev osebnih podatkov, da se omeji ali prepreči njihova nadaljnja obdelava.

USTNA ALI DRUGA OSEBNA PRIVOLITEV – je ustno ali s telekomunikacijskim ali z drugim ustreznim sredstvom ali na drug ustrezen način dana privolitev, iz katere je mogoče nedvomno sklepati na posamezno privolitev.

ANONIMIZIRANJE – je takšna sprememba oblike osebnih podatkov, da jih ni mogoče več povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa.

OBČUTLJIVI OSEBNI PODATKI – so podatki o rasnem, narodnem, narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške; občutljivi osebni podatki so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s katero od prej navedenih okoliščin.

2.1 ZASEBNOST KOT TEMELJNA ČLOVEKOVA PRAVICA

Ker se zasebnost smatra za temeljno človekovo pravico, je zaščitena z več mednarodnimi akti, predvsem pa s *Splošno deklaracijo človekovih pravic*, ki jo je sprejela in razglasila Generalna skupščina združenih narodov 10. decembra 1948. leta:
»Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.«

Vendar pa zasebnost ni enodimenzionalen pojem. Čebulj tako navaja tri sestavine zasebnosti:

- zasebnost v prostoru (možnost posameznika, da je sam);
- zasebnost osebnosti (svoboda misli, opredelitve, izražanja);
- informacijska zasebnost (možnost posameznika, da obdrži informacije o sebi, ker ne želi, da bi bili z njimi seznanjeni drugi).

Prvi dve sestavini zasebnosti spadata med temeljne človekove pravice in svoboščine in v demokratični družbi nista sporni. Kritična oz. v informacijski družbi potencialno

ogrožena pa je tretja sestavina zasebnosti, ki vključuje tudi varstvo osebnih podatkov.

V moderni družbi, ki je prežeta z informacijsko in komunikacijsko tehnologijo je najbolj na udaru ravno informacijska zasebnost. Bistvena sestavina zaščite informacijske zasebnosti je zato »kontrola pretoka in posredovanja podatkov, ki se nanašajo na nekega posameznika« (Raab, 1997, str. 158).

Ker država oz. njene institucije potrebujejo informacije za učinkovito uravnavanje življenja posameznikov ter dobro funkcioniranje družbe, jim posameznik zbiranja ne more oz. včasih celo ne sme preprečiti. Je pa zato bistvena *transparentnost uporabe* osebnih podatkov. Mellors ugotavlja: »Najboljša zaščita ni ta, da oni (država) vedo *manj* o nas, pač pa da mi vemo *več* o njih: da vemo, kaj vedo o nas in kako te informacije o nas uporabljajo.« (Raab, 1997, str. 158).

Pravica do zasebnosti se zato danes opredeljuje kot "pravica posameznika, da zahteva, da se podatki in informacije o njegovih zasebnih razmerjih ne sporočajo komurkoli" (Čebulj, 1992, str. 7) - to pomeni: tistim, ki za uporabo določene informacije niso pooblaščeni.

3 ZGODOVINA VARSTVA OSEBNIH PODATKOV

Prve potrebe po zaščiti zasebnosti ljudi so se pojavile zaradi različnih žalitev, napadov, prisluškovanj in podobno. Razlog, da se je ta pravica pričela pozno uveljavljati in izvajati v pravnih sistemih, pa je v tem, da so večino modernih kršitev zasebnosti, kot so prisluškovanje pogovorom prek telefonov, mikrofonov in elektronskih ojačevalcev, zbiranje, shranjevanje in iskanje informacij z video kamerami, računalniki in podobno, začele omogočati šele nove tehnologije. Pred njihovimi iznajdbami je bil posameznik lahko utemeljeno prepričan, da mu v zasebnem prostoru ni mogoče prisluškovati. Tudi vdor v zasebnost večje skupine oseb je bil pred uporabo računalniških baz veliko težavnejši, saj so bile informacije o posameznikih pogosto raztresene in težko dostopne.
Pravno prepoznavo je pravica do zasebnosti dobila precej pozno. Prva publikacija, ki je obravnavala to področje, izvira iz ZDA. Gre za članek dveh sodnikov ameriškega vrhovnega sodišča Warrena in Brandeisa, Pravica do zasebnosti, ki je bil objavljen leta 1890 (4 Harvard L. R., 193). Kljub temu je prišlo do kodifikacije te pravice šele 1960, ko je Prosser izdal članek pod naslovom Zasebnost (48 Cal. L. Rev., 383), leta 1977 pa je kodifikacijo opredelil v ponovni izdaji civilnih deliktov.

Znamenita fraza »to be let alone« oziroma »pustiti pri miru« pa ima bistveno daljšo zgodovino. Leta 1834 je v primeru Wheaton proti Peters ameriško vrhovno sodišče menilo, da obtoženec nič ne sprašuje in nič ne želi, razen da se ga pusti pri miru (»defendant asks nothing – wants nothing, but to be let alone …«), dokler se ne dokaže, da je kršil pravice drugega. Pravica »pustiti pri miru« je med drugim prišla močno do veljave tudi v razvpitem primeru Olmstead v ZDA. To je bil prvi primer prisluškovanja, ki ga je obravnavalo ameriško vrhovno sodišče. Po tem se je omenjena fraza uveljavila kot definicija pravice do zasebnosti, kasneje pa je dobila še nov pomen, povezan s kršenjem zasebnosti posameznika s strani države.

3.1 RAZVOJ VARSTVA OSEBNIH PODATKOV

Ko govorimo o varstvu osebnih podatkov in informacijski zasebnosti ne moremo mimo vloge in ogromnih zaslug mednarodnih organizacij. 12. člen Splošne deklaracije človekovih pravic, ki jo je sprejela Generalna skupščina združenih narodov 10. 12. 1948, določa, kot že omenjeno, da se nikogar ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Poleg tega določa tudi, da ima vsakdo pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.

Navedena deklaracija je bila sprejeta v okviru Organizacije združenih narodov (OZN)[1].

Generalni sekretar OZN je leta 1974 za Ekonomski in socialni svet združenih narodov pripravil poročilo z naslovom »Človekove pravice in znanstveni in tehnološki razvoj - Uporaba elektronike, ki lahko vpliva na pravice oseb in omejitve, ki bi morale biti podane v demokratični družbi«. To poročilo je pomembno iz dveh vidikov:

- državam, ki še nimajo zakonske ureditve varstva informacijske zasebnosti posameznika priporoča, naj le-to čimprej sprejmejo;
- vsebuje temeljne zahteve, ki naj bi jih države upoštevale pri zakonskem urejanju varstva informacijske zasebnosti.

Zadnji dokument, ki je bil sprejet v okviru OZN in se nanaša na varstvo informacijske zasebnosti, so Smernice o avtomatiziranih zbirkah osebnih podatkov. Te se v veliki meri zgledujejo po načelih, ki so se izoblikovala v okviru drugih mednarodnih, zlasti pa evropskih integracijskih oblik.

Ostale organizacije, ki so se največ ukvarjale s problematiko varstva informacijske zasebnosti, so že v prejšnjem poglavju omenjene Organizacija za ekonomsko sodelovanje in razvoj (OECD), Svet Evrope in Evropska skupnost. Najpomembnejši dokument, sprejet v okviru OECD, so prav tako že omenjene Smernice OECD, sprejete leta 1980.

V okviru Sveta Evrope je potrebno najprej omeniti Evropsko konvencijo o človekovih pravicah[2] iz leta 1953. Ta v osmem členu določa, da ima vsakdo pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in korespondence. S strani oblasti so dopustni posegi v to pravico samo, če je poseg skladen z zakonom, če je v interesu nacionalne varnosti, javne varnosti ali ekonomske koristi države in če se z njim preprečuje nered ali kriminal, se varuje zdravje, morala ali pravice in svoboščine drugih posameznikov. S to konvencijo je bilo ustanovljeno tudi Evropsko sodišče za človekove pravice (19. člen).

Na tej podlagi je bila leta 1981 sprejeta Konvencija o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov. Glavni del te konvencije sestavljajo načela, ki so opisana v prejšnjem poglavju, prispevala pa naj bi k poenotenju nacionalnih ureditev in s tem enakemu varstvu posameznikov, glede na bivališče in državljanstvo.

Naslednja omenjena organizacija je Evropska skupnost. Ta je leta 1990 sprejela predloge treh direktiv. Prvi predlog se po zgledu Sveta Evrope nanaša na varstvo

[1] Organizacija združenih narodov je mednarodna organizacija, katere članice so skoraj vse države sveta, ustanovljena pa je bila leta 1945 v San Franciscu. Med ustanovnimi članicami je bila tudi Demokratična federativna Jugoslavija. Nasledila je Ligo narodov (oz. Društvo narodov). Slovenije je članica OZN od 22. 05. 1992.

[2] Konvencija o varstvu človekovih pravic in temeljnih svoboščinah Sveta Evrope (EKČP), UL RS, št. 33/94, MP, št. 7/94.

posameznikov z vidika procesiranja osebnih podatkov. Predlog druge direktive vsebuje specifične zahteve glede varstva zasebnosti v okviru javnih digitalnih komunikacijskih omrežij, še posebej v zvezi z digitalizirano mrežo integriranih storitev in javnimi digitalnimi prenosnimi omrežji. Predmet tretjega predloga direktive pa je razvoj globalne strategije na področju zavarovanja oz. informacij, katere namen je zagotoviti uporabnikom elektronsko shranjenih, procesuiranih in prenašanih podatkov in z njimi povezanih informacijskih sistemov, zaščito pred naključnimi ali namernimi vdori in zlorabami (Čebulj, 1992, str. 11-14).

3.2 PRVA NACIONALNA ZAKONODAJA NA PODROČJU VARSTVA OSEBNIH PODATKOV

Prvi nacionalni zakon, namenjen varstvu osebnih podatkov, je sprejela Švedska, in sicer leta 1973. Vendar to ni bil prvi zakon, ki je urejal varstvo posameznikove informacijske zasebnosti. Prvi zakon na tem področju je sprejela Zvezna republika Nemčija, oz. njena federalna enota, dežela Hessen, v letu 1970. V ZDA je bil takšen zakon sprejet 1974, vendar pa obstajajo v ZDA, Kanadi in Avstraliji določene specifičnosti, ki izvirajo iz posebnosti anglosaksonskega prava in dediščine angleškega »common law«.

Poglavitne značilnosti normativnih ureditev varstva informacijske zasebnosti evropskih držav lahko strnemo v naslednje točke:

- varstvo osebnih podatkov se ureja z zakonom;
- zakonodaja je usmerjena na varstvo zasebnosti subjektov zasebnega prava;
- enako varstvo lastnim in tujim državljanom;
- zakonodaja obravnava računalniške in ročno vodene zbirke podatkov;
- zakonsko varstvo ne obravnava le zbiranja podatkov, marveč tudi obdelovanje, shranjevanje, prenos in brisanje;
- natančno definiranje pojmov;
- oblikovanje posebnih neodvisnih teles, ki spremljajo stanje na področju varstva informacijske zasebnosti;
- strogost glede izjem;
- določene formalnosti glede vzpostavitve zbirk osebnih podatkov, namene in vsebino;
- svoboden prenos podatkov prek državnih meja;
- posameznikom daje ustrezno pravno sredstvo.

4 NORMATIVNA UREDITEV

Kot že rečeno, je Slovenija, kot članica EU, OZN in drugih mednarodnih organizacij in forumov, zavezana ne le k spoštovanju svojih pravnih aktov, ki urejajo varstvo osebnih podatkov, marveč tudi k spoštovanju določb mnogih mednarodnih konvencij, pogodb, direktiv in ostalih pravnih aktov. Mednarodni akti so tako postali obvezujoča in neobvezujoča podlaga za sprejemanje novih nacionalnih aktov, ki so slovensko pravno prakso na tem področju približali mednarodni, predvsem evropski.
V tem poglavju so opisani najpomembnejši akti, tako nacionalni kot mednarodni.

4.1 KONVENCIJA O VARSTVU POSAMEZNIKOV GLEDE NA AVTOMATSKO OBDELAVO PODATKOV

Konvencija o varstvu posameznikov glede na avtomatsko obdelavo podatkov je bila sprejeta v okviru Sveta Evrope 28. 01. 1981 v Strasbourgu, njene določbe pa se v Sloveniji uporabljajo neposredno. Veljati je začela leta 1985, Slovenija pa jo je ratificirala 1994[3].
Temeljni namen Konvencije 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 pravic do zasebnosti glede na avtomatsko obdelavo osebnih podatkov, vendar pa državam članicam dopušča možnost, da ob podpisu ali kadarkoli kasneje generalnemu sekretarju Sveta Evrope med drugim predložijo tudi izjavo, da bodo zagotovile uporabo te Konvencije tudi za tiste zbirke osebnih podatkov, ki niso vodene avtomatsko.
Konvencija je sestavljena iz preambule in sedem poglavij.
Prvo poglavje opredeljuje predmet in namen Konvencije, definira izraze ter določa obseg Konvencije.
V drugem poglavju so opisana temeljna načela, ki jih bom bolj podrobno predstavil, saj je to najpomembnejše poglavje Konvencije.
Tretje poglavje ureja področje prenosa osebnih podatkov čez državne meje in v zvezi s tem postavlja v ospredje načelo prostega pretoka podatkov. Pogodbenica tako ne more, samo zaradi zaščite zasebnosti, prepovedati prenosa osebnih podatkov čez nacionalne meje na ozemlje druge pogodbenice. Prenos je lahko omejen v obsegu, kolikor njena zakonodaja vsebuje posebne ureditve za določene kategorije osebnih podatkov ali avtomatskih zbirk. Omejitve so dopustne takrat, ko gre za prenos podatkov z ozemlja pogodbenice čez ozemlje države, ki ni pogodbenica.
V četrtem poglavju je predpisano medsebojno sodelovanje med pogodbenicami. V okviru te pomoči je predpisana pomoč dajalcem podatkov, nastanjenih v tujini.

[3] Zakon o ratifikaciji Konvencije o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov, ki je bila ratificirana in objavljena leta 1994 (UL RS, št. 11/1994, Mednarodne pogodbe, št. 3/1994).

Predpisani so tudi zaščitni ukrepi v okviru pomoči, ki jo daje pooblaščeni organ. Glede stroškov je določeno, da stroški ne morejo biti večji od stroškov plačil, potrebnih za izvedence in tolmače. Stroške krije pogodbenica in ne morejo biti preneseni na posameznika.
Peto poglavje predpisuje ustanovitev posvetovalnega odbora, v katerega bo vsaka pogodbenica imenovala po enega člana in enega namestnika. Tiste članice Sveta Evrope, ki niso pogodbenice, imajo pravico, da imajo v odboru opazovalce. Posvetovalni odbor lahko daje predloge za pospešitev ali izboljšanje uporabe Konvencije, daje predloge za njeno dopolnitev, oblikuje mnenje o vsakem predlogu za dopolnitev ter na zahtevo posamezne pogodbenice lahko da mnenje o vsakem vprašanju, ki se nanaša na uporabo te konvencije.
V šestem poglavju je določen postopek za dopolnitev te Konvencije, v sedmem pa je v okviru končnih določb opredeljena njena veljavnost.

4.1.1 Načela v Konvenciji Evropskega sveta o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov

Sestavljalci Konvencije so pri oblikovanju njenega besedila izhajali iz cilja spoštovanja zakonitosti in temeljnih človekovih pravic in svoboščin. Pri tem so se zavedali, da je mednarodni pretok podatkov nujen in zato ne smejo postavljati ovir, ki bi le-tega zaustavljale, potrebno pa je bilo urediti temeljna načela, ki bi posamezniku zagotovila spoštovanje njegove zasebnosti. Konvencija je sestavljena iz sedmih delov, najpomembnejši je drugi, ki je uredil področje, ki vsebuje temeljna načela zaščite podatkov.

Prvo načelo, ki ga vsebuje Konvencija, je načelo kvalitete (kakovosti) podatkov. To načelo vsebuje pet zahtev, ki jih je potrebno spoštovati pri avtomatični obdelavi osebnih podatkov, bistvo le-teh pa je:

- podatki morajo biti pridobljeni in obdelani na zakonit način;
- namen shranjevanja in uporabe mora biti jasen;
- podatki ne smejo biti prekomerni, glede na namen, za katerega se zbirajo;
- podatki morajo biti točni;
- oblika shranjevanja podatkov mora biti določena.

Konvencija vsebuje tudi posebno načelo o prepovedi obdelovanja določenih kategorij podatkov. Osebnih podatkov, ki kažejo na rasno poreklo, versko prepričanje, religiozna ali druga verovanja, ter zdravstveno ali seksualno življenje, ni dovoljeno obdelovati, če nacionalna zakonodaja ne določa primernega varstva. Enako velja glede osebnih podatkov, ki se nanašajo na kazenske obsodbe.

Posebej je obravnavano načelo zavarovanja podatkov (t. i. »data security«). To zavezuje podpisnice, da predpišejo ustrezne ukrepe, tako organizacijske kot tehnične narave, za zaščito osebnih podatkov, shranjenih v avtomatskih zbirkah podatkov, s katerimi se preprečuje slučajno ali nepooblaščeno uničenje podatkov ali njihova

izguba, kakor tudi nepooblaščen vpogled, obdelava, spreminjanje in širjenje podatkov.

Z načelom odprtosti in načelom udeležbe oz. sodelovanja ljudi, se odražajo zahteve, da mora biti vsaki osebi omogočeno:

- da se seznani z obstojem posamezne zbirke, ki vsebuje osebne podatke, njenimi nameni in sedežem upravljavca;
- da dobi v razumnem času in brez večjih zamud in stroškov potrdilo o tem, kateri podatki, ki se nanašajo nanj, so shranjeni v določeni zbirki podatkov;
- da zahteva popravo ali izbris podatkov, če so bili obdelovani v nasprotju s pravili, vsebovanimi v nacionalni zakonodaji;
- da ima ustrezno sredstvo (zahtevo, pritožbo, ugovor), če zahtevi za potrdilo, sporočilo, popravek ali izbris ni ustreženo.

V naslednjem načelu Konvencija dopušča izjeme glede uporabe prikazanih načel in z njimi povezanih omejitev pravic posameznika, ki mu jih zagotavlja ureditev varstva osebnih podatkov. Izjeme in njihova uporaba so natančno določeni in našteti. Konvencija dopušča omejitve zaradi zaščite državne varnosti, javne varnosti, denarnih interesov države ali zatiranja kriminala in zaščite dajalcev podatkov ali pravic in svoboščin drugih oseb.

Načelo odgovornosti je v Konvenciji izraženo v obveznosti udeleženk, da v nacionalni zakonodaji določijo pravice in obveznosti upravljavcev in uporabnikov podatkov ter sankcije za primere kršitev obveznosti.

Glede načela o široki razlagi odločb Konvencije določa, da nobenega od naštetih načel ni mogoče razlagati omejujoče oz. tako da bi kakorkoli ovirala udeleženke, da zagotovijo posameznikom, na katere se nanašajo podatki, še širšo zaščito od tiste, ki jo kot minimalno določa Konvencija (Čebulj, 1990, str. 5-14).

Omeniti velja še načelo svobodnega pretoka podatkov, ki je obravnavano v tretjem delu Konvencije. S tem je določeno, da posamezna udeleženka ne more samo zaradi doseganja namena varovanja zasebnosti prepovedati ali izpostaviti posebni avtorizaciji iznosa osebnih podatkov prek nacionalnih meja na teritorij druge udeleženke. Vendar pa vsaka udeleženka lahko omeji prenos v tolikšnem obsegu, kot njena zakonodaja vsebuje posebne ureditve za določene kategorije osebnih podatkov ali avtomatskih zbirk podatkov, ki take podatke vsebujejo, zaradi narave teh kategorij podatkov ali zbirk. Tega pa ne more storiti, če zakonodaja druge udeleženke določa ekvivalentno varstvo (Čebulj, 2005, str. 26).

4.2 DIREKTIVA O VARSTVU POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV IN O PROSTEM PRETOKU PODATKOV[4]

Direktiva ima dva integralna dela. Prvi je uvodni oz. pojasnjevalni in ima 72 točk. Sestavljen je iz treh vsebinskih sklopov:

- Preambula,
- Opredelitev temeljnih ciljev,
- Pojasnjevalni (interpretacijski) napotki.

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

V prvem poglavju z naslovom Splošne določbe so opredeljeni cilji tega predpisa, glavne definicije, področje učinkovanja Direktive ter uporaba nacionalnega prava. Direktiva se nanaša tako na avtomatsko obdelavo, kot tudi na t. i. klasično obdelovanje osebnih podatkov. Prav tako so določene natančne izjeme oz. situacije, v katerih se Direktiva ne uporablja.

Najdaljše je drugo poglavje, ki se nanaša na opredelitev pojmov za zakonitost obdelovanja osebnih podatkov. To poglavje je razdeljeno na devet oddelkov, ki so v bistvu tudi načela.
Prvo je načelo zakonitosti, ki določa, da je obdelava osebnih podatkov zakonita samo, če posameznik vanjo nedvoumno privoli, v drugih primerih pa je to mogoče:

- če ima upravljalec zbirke podatkov za to pooblastilo v zakonu, če je obdelava nujna za izpolnitev njegovih nalog ali če je nujna zaradi varstva javne koristi;
- če je obdelava nujna zaradi varstva posameznika, na katerega se podatki nanašajo;
- če je obdelava nujna zaradi izvrševanja pravnih poslov, v katerih je udeležen posameznik.

Načelo predhodne določitve namena zahteva, da se podatki obdelujejo praviloma samo za vnaprej eksplicitno določene namene.
Načelo relavantnosti preprečuje prekomernost pri zbiranju osebnih podatkov, saj zahteva sorazmerje med količino zbranih podatkov in namenom njihove obdelave – zbirajo se le nujno potrebni podatki.
Načelo kvalitete podatkov zahteva točnost zbranih podatkov in, kadar je to potrebno, njihovo popolno ažurnost.
Načelo časovne omejitve pa omejuje shranjevanje osebnih podatkov v obliki, ki omogoča identifikacijo posameznika na čas, ki je nujno potreben za dosego namena, za katerega so bili podatki zbrani.

[4] Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne, 24. oktober 1995, o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem toku takih podatkov, UL Evropskih skupnosti, št. L281, 23. 11. 1995.

Načelo zavarovanja govori o tehničnih in drugih ukrepih, s katerimi naj bi se nepooblaščenim uporabnikom preprečil dostop do podatkov.
Načelo svobodnega pretoka prek državnih meja izhaja iz zahtev skupnega evropskega trga po svobodnem pretoku blaga, storitev, oseb in kapitala. V okviru tega so prikazana tudi izhodišča za skupni evropski informacijski trg.
Načelo notifikacije od držav članic zahteva, da v nacionalni zakonodaji upravljalcu zbirke osebnih podatkov naložijo obveznost, da morajo za to določeni državni organ obvestiti o tem, da bodo pričeli z obdelavo določene vrste podatkov za določene namene.
Načelo seznanjenosti posameznika zavezuje države članice, da predpišejo obveznost upravljavcu zbirke podatkov, da posameznika seznani z zbiranjem in obdelavo podatkov (Čebulj, 1996, str. 237-239).

Drugo poglavje poleg tega določa tudi izjeme in omejitve, pravico posameznika do ugovora in obveznost uradnega obveščanja nadzornega organa.

Tretje poglavje se nanaša na določitev pravnega sredstva, odgovornosti in sankcij v nacionalnih zakonodajah. Države članice morajo vsakomur zagotoviti pravico do sodnega varstva v primeru kršitev določb predpisov o varstvu osebnih podatkov. Prav tako morajo države članice posamezniku zagotoviti pravico do odškodnine v primeru nastanka škode zaradi kršitev informacijske zasebnosti. Direktiva države članice tudi zavezuje, da v svoji zakonodaji določijo ustrezne pravne sankcije za primere kršitev informacijske zasebnosti posameznika.

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

Peto poglavje se nanaša na spodbujanje priprav kodeksov ravnanja pri obdelovanju osebnih podatkov, katerih namen je prispevati k pravilnemu izvajanju nacionalnih predpisov, ki so jih sprejele države članice v skladu s to Direktivo, ob upoštevanju značilnosti različnih področij.

Šesto poglavje določa obveznost ustanovitve dveh organov za varstvo informacijske zasebnosti posameznika: nadzornega organa na nacionalnem nivoju ter delovnega telesa za varstvo posameznika z vidika obdelovanja osebnih podatkov na nivoju Evropske unije.

V sedmem poglavju Direktiva predvideva ustanovitev posebnega odbora, čigar skrb je pomoč Komisiji Evropske unije pri sprejemanju operativnih ukrepov za izvajanje vsebine te Direktive.

V končnih določbah je določeno, da morajo države članice sprejeti vse potrebne ukrepe za uskladitev notranje zakonodaje s to Direktivo v treh letih od njenega sprejema. Države morajo Komisiji Evropske unije posredovati tekste nacionalnih predpisov, ki jih sprejemajo s ciljem uskladitve s to Direktivo. Komisija je prav tako zavezana, da mora v določenih intervalih poročati Svetu Evropske unije in Evropskemu parlamentu o problemih implementacije Direktive ter ob teh poročilih pripravljati tudi ustrezne dodatne predloge in morebitne amandmaje k Direktivi. Z vidika spremljanja razvoja informacijske tehnologije je Komisija Evropske unije zadolžena tudi za proučevanje združljivosti Direktive z vidika obdelovanja posebnih osebnih podatkov – »zvokov in podob«[5], ki se nanašajo na fizično osebo.

4.3 USTAVA RS KOT NEPOSREDNA PODLAGA ZA ZAKONSKO UREDITEV VARSTVA OSEBNIH PODATKOV

Varstvo osebnih podatkov je v Republiki Sloveniji ena izmed ustavno zagotovljenih človekovih pravic in temeljnih svoboščin in spada v okvir pravic s področja zasebnosti. Med te pravice prištevamo še pravico do osebnega dostojanstva (34. člen Ustave RS), varstvo pravic zasebnosti in osebnostnih pravic (35. člen Ustave RS), nedotakljivost stanovanja (36. člen), varstvo tajnosti pisem in drugih občil (37. člen), svobodo izražanja (39. člen) ter svobodo vesti (41. člen).

Ustava RS v 38. členu vsakomur zagotavlja varstvo osebnih podatkov, ki se odraža v zahtevi po zakonitosti zbiranja, obdelave in uporabe osebnih podatkov in v zahtevi po njihovemu zbiranju in uporabi za vnaprej določene namene, posamezniku pa daje pravici do seznanjenosti o tem, kateri podatki se zbirajo, in do sodnega varstva. Gre za pravico, katere cilj ni varstvo podatkov samo po sebi, temveč je namen pravice pravzaprav varstvo posameznika, na katerega se podatki nanašajo. Ustava zato prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja, zbiranje, obdelavo, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa za predmet zakonskega urejanja in vsakomur daje pravico, da se seznani z zbranimi osebnimi podatki, ki se nanašajo nanj, za primer zlorabe pa tudi pravico do sodnega varstva. V tem členu lahko razberemo štiri načela:

- načelo zakonitosti,
- načelo namenskosti (oziroma načelo predhodne določitve namena),
- načelo seznanjenosti,
- načelo sodnega varstva.

Najpomembnejše je gotovo načelo zakonitosti. S tem se seveda ne želi zmanjševati pomena ostalih načel, dejstvo pa je, da z vidika ustavnopravne presoje največkrat pride v poštev prav omenjeno načelo, ostala tri pa se nanj tesno navezujejo.

[5] Sound and image.

Zakonodajalec mora zagotoviti njihovo izvajanje, je pa tudi edini, ki lahko predpiše odstopanja od teh načel (Vintar in Grad, 2004, str. 249).

Načelo zakonitosti seveda ne izključuje dopustnosti zbiranja, obdelovanja in uporabe podatkov na podlagi soglasja osebe, na katero se podatki nanašajo, pač pa to načelo zahteva, da so primeri in pogoji za zbiranje in uporabo podatkov na podlagi soglasja opredeljeni z zakonom. Iz soglasja mora biti razvidno, za katere podatke je soglasje dano, pa tudi za katere namene se lahko uporabljajo.

Ustavodajalec se je odločil za tako imenovani »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 tega, kar je izrecno dovoljeno z zakonom. Vsaka obdelava osebnih podatkov pomeni poseg v ustavno varovano človekovo pravico, zaradi tega je takšen poseg dopusten, če je v zakonu opredeljeno, kateri podatki se smejo obdelovati, jasno pa mora biti razviden tudi namen obdelave osebnih podatkov ter zagotovljeno ustrezno zavarovanje.

4.4 ZAKON O VARSTVU OSEBNIH PODATKOV (ZVOP-1)

Prvi zakon s področja varstva osebnih podatkov v Republiki Sloveniji je bil Zakon o varstvu osebnih podatkov[6], ki je začel veljati 24. 03. 1990. Njegov temeljni cilj je bil urediti varstvo osebnih podatkov in v tem okviru preprečiti nezakonite in čezmerni posege v integriteto človekove osebnosti, ki so lahko posledica zbiranja, obdelave, shranjevanja, in posredovanja osebnih podatkov ter njihove uporabe.
Zaradi približevanja Evropski uniji in zahtev direktive 95/46/ES Evropskega parlamenta in Sveta o zaščiti posameznikov pri obdelavi osebnih podatkov in o prostem gibanju podatkov je Državni zbor Republike Slovenije 08. 07. 1999 sprejel nov Zakon o varstvu osebnih podatkov[7], ki je začel veljati 07. 08. 1999. Novi zakon naj bi bil že usklajen z Direktivo, vendar pa se je izkazalo, da je pomanjkljiv, zato je bil leta 2001 sprejet Zakon o spremembah in dopolnitvah Zakona o varstvu osebnih podatkov[8], ki je začel veljati 24. 07. 2001. Namen novele je bil predvsem v uskladitvijo z Direktivo v določbah, ki se nanašajo na neodvisni nadzorni organ za varstvo osebnih podatkov.
Zadnji, sedaj veljavni, Zakon o varstvu osebnih podatkov[9], ki je bil sprejet 15. 07. 2004 in začel veljati 01. 01. 2005, je bil potreben predvsem zaradi določb evropskega pravnega reda, spet Direktive, saj je sodna praksa Sodišča Evropskih skupnosti leta

[6] UL RS, št. 8/1990, ZVOP.
[7] UL RS, št. 59/1999, ZVOP.
[8] UL RS, št. 57/2001 in 59/2001 – popravek.
[9] UL RS, št. 86/2004, ZVOP-1.

2003 ugotovila, da so nekatere vsebine določb tako podrobne, da jih morajo države članice sprejeti z natanko tako vsebino.

ZVOP-1 je podrobno opisan v nadaljevanju.

4.4.1 Splošne določbe - I. DEL (1.-7. člen)

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

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

Načelo zakonitosti in poštenosti je primarno in najpomembnejše načelo, po katerem se morajo osebni podatki obdelovati zakonito in pošteno.

Načelo sorazmernosti določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.

Načelo prepovedi diskriminacije zagotavlja varstvo osebnih podatkov vsakemu posamezniku ne glede na raso, barvo kože, veroizpoved, etično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, premoženjsko stanje, rojstvo, izobrazbo, družbeni položaj, državljanstvo, kraj oz. vrsto prebivališča ali katerokoli drugo osebno okoliščino.

V petem členu je določena ozemeljska veljavnost ZVOP-1. V dikcijo tega člena je implementiran 4. člen Direktive 95/46/ES, ki določa pogoje za uporabo nacionalne zakonodaje.

Nadalje je razložen pomen izrazov, uporabljenih v tem zakonu, našteti pa so že na začetku te diplomske naloge. Poznavanje teh izrazov je seveda bistveno za razumevanje določb tega zakona in ostalih aktov s tega področja.

V sedmem členu so določene izjeme glede uporabe vseh ali dela določb tega zakona v določenih življenjskih situacijah, kjer bi bilo določbe tega zakona nesmiselno uporabljati. Teh izjem je sedaj manj, poleg tega pa se tudi precej razlikujejo od izjem, ki jih je določal ZVOP iz leta 1999[10]. ZVOP-1 določa tri skope izjem:

- Prvi sklop se nanaša na obdelavo osebnih podatkov, ki jih posamezniki obdelujejo izključno v okviru svojega zasebnega življenja. V primeru izjem iz tega odstavka je izključena uporaba celotnega zakona.
- Drugi sklop izjem se nanaša na osebne podatke, ki jih v svojih členih obdelujejo politične stranke, sindikati in verske skupnosti. V teh primerih se ne uporabljajo določbe 26., 27. in 28. člena tega zakona.
- Tretja izjema pa se nanaša na osebne podatke, ki jih za namene obveščanja javnosti obdelujejo mediji. Ta odstavek izključuje uporabo določb drugega odstavka 25. člena, 26., 27. in 28. člena ter V. dela zakona.

4.4.2 Obdelava osebnih podatkov – II. DEL (8.–28. člen)

Drugi del zakona je razdeljen na štiri poglavja.

Začne se s splošno določbo glede določanja dopustne pravne podlage za obdelavo osebnih podatkov. Osebne podatke in njihovo obdelavo določa zakon ali pa mora biti podana posameznikova privolitev. Nadalje je natančno razdelana pravna podlaga za obdelavo osebnih podatkov v javnem in zasebnem sektorju ter določene izjeme splošnih pravnih podlag, kar je v skladu z določbami Direktive 95/46/ES. Zakon v nadaljevanju določa, da mora biti posameznik, na katerega se nanašajo osebni podatki, predhodno pisno ali na drug ustrezni način seznanjen z namenom njihove obdelave.
Osmi člen ZVOP-1 tako neposredno konkretizira drugi odstavek 38. člena Ustave RS.

Upravljalec osebnih podatkov lahko posamezna opravila v zvezi z obdelavo podatkov s pogodbo zaupa pogodbenemu obdelovalcu. Pomembno pri tem je, da lahko obdelovalec osebnih podatkov podpiše pogodbo le s pravno osebo ali zasebnikom, ki izpolnjuje pogoje iz 24. člena ZVOP-1:

- pogodbeni obdelovalec mora biti registriran za opravljanje takšne dejavnosti;
- zagotavljati mora ustrezne organizacijske, tehnične in logično-tehnične postopke;
- medsebojne pravice in obveznosti morajo biti sklenjene v pogodbi, ki mora biti pisna.

[10] UL RS, št. 59/2001 in 59/2001, ZVOP.

V tem delu je podana tud neposredna podlaga za obdelavo osebnih podatkov v tistih primerih in življenjskih situacijah, ko je obdelava podatkov nujna za varovanje posameznikovega življenja ali telesa. V teh primerih se osebni podatki lahko zbirajo ne glede na to, da za obdelavo osebnih podatkov druga zakonita pravna podlaga ne obstaja. V teh primerih ZVOP-1 presega okvire sistemskega zakona in že sam nudi zadostno pravno podlago za ukrepanje.

Občutljivi osebni podatki so najsubtilnejša kategorija osebnih podatkov, definirani so v šestem členu ZVOP-1, v tem delu zakona pa je taksativno določenih osem pravnih podlag, ki dopuščajo njihovo obdelavo. Podlaga za določbo 13. člena ZVOP-1 je določba 8. člena Direktive 95/46/ES, ki določa obdelavo občutljivih osebnih podatkov. Tam je zapisano, da države članice prepovedujejo obdelavo osebnih podatkov, ki kažejo na rasni ali etični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu in obdelavo osebnih podatkov v zvezi z zdravjem ali spolnim življenjem.
Glede na to, da pomeni razkritje teh podatkov hud poseg v zasebnost posameznika, na katerega se podatki nanašajo, je treba zavarovanju obdelave občutljivih podatkov posvetiti še posebno pozornost.
ZVOP-1 v nadaljevanju obravnava avtomatizirano obdelavo podatkov, pri tem pa izrazito ščiti posameznika, ki je v obdobju modernih informacijskih tehnologij postal vse prevečkrat objekt obdelave, zavedati pa se je tudi treba, da je nevarnost zlorabe informatike pri oblikovanju odločitev ena glavnih nevarnosti, ki nam grozi v prihodnosti.
Osebni podatki se lahko zbirajo le za določene in zakonite namene, zakon pa določa še, da se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače. Tu je vsebovano eno od temeljnih načel varstva osebnih podatkov – načelo namenskosti.

V tem delu je urejeno tudi vodenje evidenc. Upravljavcu se nalaga, da za vsako zbirko osebnih podatkov, ki jo vodi in vzdržuje, vzpostavijo katalog zbirke osebnih podatkov. Pri tem ni pomembno, ali se zbirka osebnih podatkov vodi na podlagi zakona, na podlagi osebne privolitve posameznika, na podlagi pogodbenega razmerja ali pa na kakšni drugi pravni podlagi iz 9. in 10. člena ZVOP-1. Natančno je določeno tudi, kaj katalog zbirke osebnih podatkov vsebuje ter da mora upravljalec skrbeti za točnost in ažurnost podatkov.
Upravljalec pristojnemu organu (Državnemu nadzornemu organu za varstvo osebnih podatkov) ni dolžan posredovati vseh podatkov iz katalogov zbirk osebnih podatkov, pač pa le tiste, ki mu jih določa 27. člen ZVOP-1, posredovati pa jih mora 15 dni pred vzpostavitvijo zbirke ali pred vnosom nove vrste osebnih podatkov.
Register zbirk osebnih podatkov, ki ga v skladu z metodologijo njegovega vodenja vodi in vzdržuje Državni nadzorni organ za varstvo osebnih podatkov, je v 13. točki prvega odstavka 6. člena ZVOP-1 definiran kot register, v katerem so podatki iz katalogov zbirk osebnih podatkov. Vsebuje torej tiste podatke, ki so jih nadzornemu organu iz svojih zbirk posredovali posamezni upravljavci. Določeno je tudi, kdo register vodi in kje ga objavi.

4.4.3 Pravice posameznika – III. DEL (29. do 36. člen)

Tretji del se začne z določbo, da mora Državni nadzorni organ vsakomur dovoliti vpogled v register zbirk osebnih podatkov ter prepis podatkov. V skladu z Zakonom o informacijskem pooblaščencu[11] je to od 31. 12. 2005 obveznost Informacijskega pooblaščenca. V skladu z tretjim odstavkom 38. člena Ustave RS je zagotovljena pravica posameznika do seznanitve z zbranimi osebnimi podatki, ki se nanašajo nanj, kot tudi pravica do sodnega varstva ob zlorabi osebnih podatkov posameznika (30. člen). V 31. členu pa je urejen postopek za uveljavljanje pravic, ki so priznane posamezniku v določbi predhodnega člena.
Pravice do dopolnitve, popravka, blokiranja, izbrisa in ugovora, so izraz pravice do informacijske samoodločbe, katere namen je zagotoviti transparentnost obdelave osebnih podatkov, s tem pa dobroverno in pošteno obdelavo osebnih podatkov. S tem se uresničuje temeljno načelo zakonitosti in poštenosti in 2. člena tega zakona.

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

4.4.4 Institucionalno varstvo osebnih pravic – IV. DEL (37. do 61. člen)

Inšpekcijski nadzor nad varstvom osebnih podatkov opravlja Državni nadzorni organ za varstvo osebnih podatkov. V zvezi z določbami o državnem nadzornem organu pa je treba opozoriti, da je 31. 12. 2005 začel veljati Zakon o informacijskem pooblaščencu (ZInfP), ki je razveljavil vse določbe 1. poglavja IV. Dela ZVOP-1, razen omenjenega 37. člena (razveljavljeni so členi od 37 do 46; vsebina teh členov je smiselno povzeta v členih od 4 do 9 ZInfP). Omenjeni zakon je združil dva organa, in sicer Pooblaščenca za dostop do informacij javnega značaja, ki je imel prej status neodvisnega organa in Inšpektorat za varstvo osebnih podatkov, ki je deloval kot organ v sestavi Ministrstva za pravosodje. Več o ZInfP v nadaljevanju.
V nadaljevanju je določeno, da varuh človekovih pravic opravlja svoje naloge na področju varstva osebnih podatkov zgolj v razmerju do enega dela javnega sektorja. Varuhova pristojnost se tako razteza le na delo državnih organov, organov samoupravnih lokalnih skupnosti in nosilcev javnih pooblastil. Nad zasebnim sektorjem varuh nima pristojnosti. Varuh v letnem poročilu državnemu zboru poroča o ugotovitvah, predlogih in priporočilih ter o stanju na področju varstva osebnih podatkov. Delovno telo državnega zbora, Odbor za notranjo politiko, javno upravo in

[11] UL RS, št. 113/2005, ZInfP.

pravosodje, spremlja razmere na področju varstva osebnih podatkov in se seznani z letnim poročilom in delom Informacijskega pooblaščenca.

4.4.5 Iznos osebnih podatkov – V. DEL (62.–71. člen)

Zakon loči med iznosom v države članice EU in Evropskega gospodarskega prostora (EGS) ter v države, ki to niso in jih zakon označuje za tretje države. Za prvo skupino velja prost pretok podatkov. To pomeni, da se v primerih, ko se osebni podatki posredujejo upravljavcu, pogodbenemu upravljavcu ali uporabniku osebnih podatkov, ki je ustanovljen, ima sedež ali je registriran v državi članici EU ali EGS, določbe zakona o iznosu podatkov ne uporabljajo.
Iznos podatkov tretjo državo pa je dopusten samo, če Državni nadzorni organ izda odločbo, s katero ugotovi, da država, v katero se iznašajo podatki, zagotavlja ustrezno raven varstva osebnih podatkov. Opisan je postopek za ugotavljanje te ravni, državni nadzorni organ pa vodi seznam držav, ki jo zagotavljajo.

4.4.6 Področne ureditve – VI. DEL (72.–90. člen)

Zakon, v nasprotju s prejšnjim, vsebuje poseben del, ki ureja področne ureditve. V okviru tega vsebuje sedem poglavij:

- neposredno trženje,
- video nadzor,
- biometrija,
- evidenca vstopov in izstopov iz prostorov,
- javne knjige,
- povezovanje zbirk osebnih podatkov,
- strokovni nadzor.

4.4.7 Kazenske določbe - VII. DEL (91.–103. člen)

Zakon vsebuje obširne prekrškovne določbe, ki se nanašajo na pravne osebe, samostojne podjetnike, odgovorne osebe pravnih oseb … Globe so precej visoke in določene v razponu.
S prekrški so sankcionirana posamezna nepravilna aktivna ravnanja in pasivnost organa, ki bi sicer moral opraviti določene aktivnosti. Prekrškovne določbe si smiselno in sistematično sledijo po posameznih delih in poglavjih zakona.

4.4.8 Prehodne in končne določbe – VIII. DEL (104.–117. člen)

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

4.5 MNENJE O ZVOP-1

Kljub temu da koncept varstva osebnih podatkov z uveljavitvijo tega zakona ostaja praktično enak kot doslej, pa se posamezne določbe novega zakona precej razlikujejo od prej veljavnih. Že kratek pogled pokaže, da je precej obsežnejši od dosedanjih zakonov, bistvena razlika pa se kaže v tem, da novi zakon ni zgolj sistemski zakon, kot so bili dotedanji, ampak v svojem VI. delu tudi tako imenovani 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, video nadzora, biometrije, evidentiranja vstopov in izstopov iz prostorov ter strokovnega nadzora.

4.6 ZAKON O DOSTOPU DO INFORMACIJ JAVNEGA ZNAČAJA

Četrti člen Zakona o dostopu do informacij javnega značaja[12] pravi, da je informacija javnega značaja informacija, ki izvira iz delovnega področja organa, nahaja pa se v obliki dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva, ki ga je organ izdelal sam, v sodelovanju z drugim organom ali pridobil od drugih oseb. Fizične in pravne osebe lahko te informacije pod določenimi pogoji uporabijo tudi za pridobitne in nepridobitne namene (ponovna uporaba informacij).
ZDIJZ določa tri kriterije, po katerih lahko opredelimo informacijo javnega značaja:

- biti mora informacija, ki izvira iz delovnega področja organa;
- organ mora z njo razpolagati;
- nahajati se mora v materializirani obliki (fizični).

Informacija mora biti povezana z delom organa, zato zanjo ne moremo šteti vsakodnevne reklame, osebnega rokovnika, koledarja, razglednice in druge oblike dokumentov, če ti ne služijo uradnemu namenu organa.
Informacija javnega značaja se lahko nanaša na kakršnokoli vsebino na vseh področjih delovanja organa, ki so povezani z njegovimi aktivnostmi ali odločitvami, ki spadajo v njegov delokrog.

[12] ZDIJZ-UPB2, UL RS, št. 51/2008.

Informacije javnega značaja so prosto dostopne pravnim ali fizičnim osebam.

Organ, ki razpolaga s konkretno informacijo, prosilcu zavrne dostop do nje, če se zahteva nanaša na:

- podatek, ki je na podlagi zakona, ki ureja tajne podatke, opredeljen kot tajen;
- podatek, ki je opredeljen kot poslovna skrivnost v skladu z zakonom, ki ureja gospodarske družbe;
- osebni podatek, katerega razkritje bi pomenilo kršitev varstva osebnih podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov;
- podatek, katerega razkritje bi pomenilo kršitev zaupnosti individualnih podatkov o poročevalskih enotah, skladno z zakonom, ki ureja dejavnost državne statistike;
- podatek, katerega razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti, skladno z zakonom, ki ureja davčni postopek;
- podatek, ki je bil pridobljen ali sestavljen zaradi kazenskega pregona ali v zvezi z njim ali postopka s prekrški in bi njegovo razkritje škodovalo njegovi izvedbi;
- podatek, ki je bil pridobljen ali sestavljen zaradi upravnega postopka in bi njegovo razkritje škodovalo njegovi izvedbi;
- podatek, ki je bil pridobljen ali sestavljen zaradi pravdnega, nepravdnega ali drugega sodnega postopka in bi njegovo razkritje škodovalo njegovi izvedbi;
- podatek iz dokumenta, ki je v postopku izdelave in je še predmet posvetovanja v organu, njegovo razkritje pa bi povzročilo napačno razumevanje njegove vsebine;
- podatek o naravni oziroma kulturni vrednoti, ki v skladu z zakonom, ki ureja ohranjanje naravne ali kulturne dediščine, ni dostopen javnosti zaradi varovanja naravne oziroma kulturne vrednote;
- podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov in bi njegovo razkritje povzročilo motnje pri delovanju oziroma dejavnosti organa.

V nadaljevanju je opredeljen katalog informacij javnega značaja. To je evidenca, ki jo mora vsak organ redno vzdrževati, jo po vsebinskih sklopih in na primeren način javno objavljati, vsakemu prosilcu pa mora biti omogočen vpogled.
Ministrstvo je dolžno redno vzdrževati in na svetovnem spletu javno objavljati državni katalog informacij javnega značaja, ki združuje informacije posameznih katalogov iz prejšnjega odstavka.

4.7 KAZENSKI ZAKONIK

Zloraba osebnih podatkov je v 154. členu Kazenskega zakonika[13] opredeljena 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. Tako se kaznuje tudi, kdor vdre v računalniško vodeno bazo podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen oseben podatek. Če dejanje stori uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let.

4.8 OSTALI ZAKONI

Za varstvo osebnih podatkov so zelo pomembni še Zakon o informacijskem pooblaščencu, Zakon o varuhu človekovih pravic in Zakon o policiji, ki pa bodo bolj podrobno obravnavani v naslednjih poglavjih.

[13] KZ-UPB1, UL RS, št. 95-4208/2004.

5 ORGANI VARSTVA OSEBNIH PODATKOV

5.1 RAZVOJ DOSTOPA DO INFORMACIJ JAVNEGA ZNAČAJA

Pravica do informiranja ima svoje korenine v zapisih stare Kitajske iz 7. stoletja. V 18. stoletju (leta 1766) je na njihovi podlagi duhovnik in član švedskega parlamenta Anders Chidenius v zakonu o svobodi tiska in dostopu do javnih dokumentov prvič opredelil pravico dostopa do javnih informacij. Ta pravica se je nato v različnih državah uveljavljala v različnih časovnih obdobjih in na različne načine. Deklaracija OZN o človekovih pravicah, ki je nastala leta 1948, je na tem področju naredila pomemben razvojni korak, saj je poleg svobode izražanja prvič opredelila tudi pravico do iskanja informacij. Pokazalo pa se je, da je pri pravici do informacij treba podrobneje in jasneje določiti vlogo države. Za Švedsko in Finsko (1919) so v drugi polovici prejšnjega stoletja države množično sprejemale zakone o dostopu do informacij javnega značaja. Danes ima t. i. zakone FOI (Freedom of Information) večina evropskih držav (izjeme so Belorusija, Rusija, Črna gora, Ciper, Luksemburg in Malta) in veliko držav drugod po svetu, skupaj 62. Kar 25 med njimi ima v teh zakonih opredeljeno uporabo testa interesa javnosti, od julija 2005 tudi Slovenija.

5.2 RAZVOJ V SLOVENIJI

Priporočila Sveta Evrope iz osemdesetih let prejšnjega stoletja in začetka tega stoletja – Recommendation (1981) 19 in Recommendation (2002) 2 – narekujejo, da države članice EU, torej tudi Slovenija, v svoji zakonodaji in praksi uredijo uresničevanje pravice dostopa do informacij javnega značaja tako, da bo lahko od organa javne oblasti vsak dobil želeno informacijo. Državni zbor Republike Slovenije je na podlagi Ustave RS iz leta 1991 februarja 2003 sprejel Zakon o dostopu do informacij javnega značaja – ZDIJZ (Ur. l. RS, št. 24/2003), ki sledi usmeritvam mednarodnih aktov in Evropske unije. Njegov namen je zagotoviti javnost in odprtost delovanja javne uprave ter vsakomur omogočiti dostop do javnih informacij, torej tistih, ki so povezane z delovnimi področji organov javne uprave.

Leta 2005 je bil z novelo Zakona o dostopu do informacij javnega značaja narejen še korak naprej. Novela je uvedla številne novosti, kot sta ponovna uporaba informacij javnega značaja in pristojnosti upravne inšpekcije na področju izvajanja tega zakona, ter prinesla tudi test javnega interesa. S tem se je Slovenija pridružila tistim demokratičnim državam, ki, kadar gre za javni interes, tudi izjeme obravnavajo s pridržkom.

V Sloveniji smo imeli do konca leta 2005 tri organe, ki so se ukvarjali z varstvom osebnih podatkov, in sicer:

- Inšpektorat za varstvo osebnih podatkov,
- Varuh človekovih pravic,
- Pooblaščenec za dostop do informacij javnega značaja.

V predlogu novega zakona, oceni stanja in razlogih za sprejem novega zakona je bila ponujena racionalnejša možnost združitev dveh ločenih organov, nadzornega organa za varstvo osebnih podatkov in pooblaščenca za dostop do informacij javnega značaja, v informacijskega pooblaščenca, ki opravlja funkcije na obeh področjih. To je bilo podprto z dvema razlogoma. Prvi je bil vsebinske narave in je izhajal iz ugotovitve, da bosta dva organa, katerih delovno področje se tako prepleta, pogosto prihajala v konflikt. Drugi pomemben razlog pa je bil vodenje enotne pravne prakse na področju dostopa do informacij javnega značaja in varstva osebnih podatkov. Enotna praksa je pomembna tako za zavezance, ki morajo slediti določilom Zakona o dostopu do informacij javnega značaja in ZVOP-1, kot tudi prosilce in »lastnike« osebnih podatkov. Do konflikta teh dveh pravic prihaja zelo pogosto in reševanje le-teh je lahko najbolj učinkovito, če znotraj enega organa, v katerem strokovnjaki poznajo obe področji, pride do poenotenja stališč.

5.3 INFORMACIJSKI POOBLAŠČENEC

Z Zakonom o Informacijskem pooblaščencu[14] je bil 31. 12. 2005 ustanovljen samostojni in neodvisni organ Informacijski pooblaščenec. Zadolžen je tako za dostop do informacij javnega značaja, kot za varstvo osebnih podatkov. S tem zakonom se v pravni red Republike Slovenije implementira določbe Direktive 95/46/ES.

V ZInfP je določeno, da je Informacijski pooblaščenec samostojen in neodvisen organ, ki je pristojen za:

- odločanje o pritožbi zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače kršil pravico do dostopa ali ponovne uporabe informacije javnega značaja ter v okviru postopka na drugi stopnji tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in na njegovi podlagi izdanih predpisov;
- inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Republike Slovenije, ter opravljanje drugih nalog, ki jih določajo ti predpisi;
- odločanje o pritožbi posameznika, kadar upravljalec osebnih podatkov ne ugodi zahtevi posameznika glede pravice posameznika do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij,

[14] ZInfP, UL RS, št. 113/05.

pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov.

V svojem uradu Informacijski pooblaščenec organizira in usklajuje delo vseh zaposlenih, vključno državnih nadzornikov za varstvo osebnih podatkov, izvaja druga pooblastila predstojnika državnega organa in opravlja inšpekcijski nadzor po ZVOP-1.

Informacijskega pooblaščenca imenuje Državni zbor RS na predlog predsednika Republike Slovenije, na to mesto pa je lahko imenovana oseba, ki izpolnjuje pogoje iz šestega člena ZInfP. Trenutno to delo opravlja Nataša Pirc Musar.

Poleg ZInfP so pristojnosti Informacisjkega pooblaščenca urejene še v:

- Zakonu o varstvu osebnih podatkov,
- Zakonu o dostopu do informacij javnega značaja,
- Zakonu o medijih[15],
- Zakonu o elektronskih komunikacijah[16],
- Zakonu o ustavnem sodišču[17] (glej 23a člen -> pristojnost IP za vlaganje Ustavnih zahtev).

5.3.1 Pristojnosti informacijskega pooblaščenca na podlagi ZVOP-1:

- izvajanje inšpekcijskega nadzora nad izvajanjem določb ZVOP-1, kar pomeni obravnavanje prijav, pritožb, sporočil in drugih vlog, v katerih je izražen sum kršitve zakona;
- odrejanje inšpekcijskih ukrepov iz 54. člena ZVOP-1 (prepoved obdelave osebnih podatkov, anonimiziranje, blokiranje, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se obdelujejo v nasprotju z zakonom);
- odrejanje drugih ukrepov iz inšpekcijskega nadzora v skladu z Zakonom o inšpekcijskem nadzoru in Zakonom o splošnem upravnem postopku (5. točka prvega odstavka 54. člena ZVOP-1);
- opravljanje preventivnega inšpekcijskega nadzora pri upravljavcih osebnih podatkov s področja javnega in zasebnega sektorja;
- vodenje in vzdrževanje registra zbirk osebnih podatkov in skrb, da je register ažuren in javno dostopen prek svetovnega spleta (28. čl. ZVOP-1);
- omogočanje vpogleda in prepisa podatkov iz registra zbirk osebnih podatkov (29. čl. ZVOP-1);
- vodenje postopkov o prekrških s področja varstva osebnih podatkov;

[15] ZMed, UL RS, št. 35/01 in Zmed – UPB1, UL RS št. 110/06.
[16] ZEKom, UL RS, št. 43/04 in ZEKom UPB1, UL RS št. 13/07.
[17] ZUstS, UL RS, št. 15/94 in ZUstS UPB1, UL RS št. 64/07.

- podajanje kazenskih ovadb oz. izvedba postopkov v skladu z zakonom, ki ureja prekrške, če pri inšpekcijskem nadzoru ugotovi sum storitve KD ali prekrška;
- odločanje o ugovoru posameznika glede obdelave osebnih podatkov na podlagi četrtega odstavka devetega člena in tretjega odstavka 10. člena ZVOP-1;
- izdajanje odločb o zagotavljanju ustrezne ravni varstva osebnih podatkov v tretjih državah (63. čl ZVOP-1);
- vodenje postopkov ugotavljanja ustrezne ravni varstva osebnih podatkov v tretjih državah na podlagi ugotovitev inšpekcijskega nadzora in drugih informacija (64. čl. ZVOP-1);
- vodene upravnih postopkov za izdajo dovoljenj o iznosu osebnih podatkov v tretjo državo (70. čl. ZVOP-1);
- vodenje upravnih postopkov za izdajo dovoljenj za povezovanje javnih financ 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;
- vodenje upravnih postopkov za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba izvajanja boimetrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1;
- sodelovanje z državnimi organi, pristojnimi organi EU 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;
- dajanje in objavljanje prehodnih mnenj državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov prepisov z zakoni in drugimi predpisi, ki urejajo osebne podatke;
- dajanje in objavljanje neobveznih mnenj o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oz. njihovih predlogov v zvezi s predpisi s področja varstva osebnih podatkov;
- pripravljanje, dajanje in objavljanje neobveznih navodil in priporočil glede varstva osebnih podatkov na posameznem področju;
- na spletni strani in na druge obvezne načine objavlja predhodna mnenja o usklajenosti predlogov zakonov in drugih predpisov z zakoni in drugimi prepisi s področja varstva osebnih podatkov ter zahtev za oceno ustavnosti predpisov (48. čl .ZVOP-1), izdajanje notranjega glasila ter strokovne literature, objavljanje odločb in sklepov sodišč, ki se nanašajo na varstvo osebnih podatkov, ter neobvezna mnenja, pojasnila, stališča in priporočila glede varstva osebnih podatkov na posameznem področju (49. čl. ZVOP-1);
- dajanje izjav za javnost o opravljenih nadzorih in pripravljanje letnih poročil o svojem delu;
- je prekrškovni organ, pristojen za nadzor nad izvajanjem Zakona o informacijskem pooblaščencu, Zakona o dostopu do informacij javnega značaja v okviru pritožbenega postopka in Zakona o varstvu osebnih podatkov.

Pri Informacijskem pooblaščencu so poleg informacijskega pooblaščenca zaposleni državni nadzorniki za varstvo osebnih podatkov. Pri opravljanju nadzora je državni nadzornik upravičen:

- pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, iznašati osebne podatke v tretjo državo in jih posredovati tujih uporabnikom;
- pregledovati vsebino zbirk in katalog zbirk osebnih podatkov ne glede na njihovo zaupnost in tajnost;
- 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;
- izvajati druge pristojnosti, določene z zakonom, ki ureja inšpekcijski nadzor, ter z zakonom, ki ureja splošni upravni postopek;
- opravljati druge zadeve, določene z zakonom, zlasti z Zakonom o inšpekcijskim nadzorstvu[18].

Informacijski pooblaščenec pri svojem delu sodeluje z drugimi državnimi organi, organi Evropske unije za varstvo osebnih podatkov, mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi na vseh področjih, ki so pomembna za varstvo osebnih podatkov.
Daje tudi predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti in drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ali predpisov z zakoni in predpisi, ki urejajo osebne podatke. Na Ustavno sodišče RS lahko vloži tudi zahtevo za oceno ustavnosti in zakonitosti predlaganih zakonov in predpisov, če se v zvezi z postopkom, ki ga vodi, pojavi vprašanje ustavnosti in zakonitosti.

Delo Informacijskega pooblaščenca je javno, zato lahko izdaja glasila in strokovno literaturo, na spletni strani objavlja predhodna mnenja, zahteve za oceno ustavnosti, potem ko jih je sprejelo Ustavno sodišče RS, ter pooblaščenčeve odločbe in sklepe, odločbe in sklepe sodišč s splošno in upravno pristojnostjo, ki se nanašajo na varstvo osebnih podatkov, daje neobvezna mnenja o skladnosti kodeksov poklicne etike, splošnih pogojih poslovanja oz. njihovih predlogih s predpisi s področja varstva osebnih podatkov. Prav tako lahko daje neobvezna mnenja, pojasnila, navodila in priporočila ter zavzema stališča o vprašanjih s področja varstva osebnih podatkov ter daje izjave za javnost o opravljenih inšpekcijskih nadzorih. O svojih aktivnostih lahko obvešča medije.

[18] Zakon o inšpekcijskem nadzorstvu, (ZIN), UL RS, št. 56/2002.

5.3.2 Pristojnosti informacijskega pooblaščenca na področju dostopa do informacij javnega značaja

Na področju dostopa do informacij javnega značaja ima Informacijski pooblaščenec pristojnosti pritožbenega organa. Pritožbeni postopek se vodi po določbah Zakona o splošnem upravnem postopku, Pooblaščenec pa lahko prosilcem za informacije pomaga:

- kadar je organ zahtevo za dostop zavrgel;
- kadar je organ izdal zavrnilno odločbo;
- kadar organ ni posredoval informacij v obliki, ki jo je zahteval prosilec.

V ZDIJZ je urejeno tudi področje ponovne uporabe informacij javnega sektorja[19], ki jo od nas zahteva Evropska unija z Direktivo EC/98/03. Informacijski pooblaščenec je pritožbeni organ tudi na področju ponovne uporabe informacij javnega sektorja.
Zakon o dostopu do informacij javnega značaja poleg zgoraj zapisanih določa še pristojnost vodenja evidence vseh podeljenih izključnih pravic na področju ponovne uporabe informacij (člen 36a, 5. odstavek).

Na področju dostopa do informacij javnega značaja ima Informacijski pooblaščenec tudi pristojnosti, ki mu jih podeljuje Zakon o medijih. 45. člen ZMed določa, da predstavniki medijev – novinarji - pridobivajo informacije za medije. Ko se odgovor na vprašanje medija nahaja v nekem dokumentu, je pravna podlaga za pritožbo v ZDIJZ, kar pomeni, da je pritožbeni organ Informacijski pooblaščenec.

5.4 VARUH ČLOVEKOVIH PRAVIC

Zakon o varstvu osebnih podatkov, poleg Informacijskega Pooblaščenca, določa tudi neodvisni nadzor nad varstvom osebnih podatkov s strani Varuha človekovih pravic.

Varuh človekovih pravic ali ombudsman je nadzornik oblasti, ki s svojimi kritikami, mnenji, predlogi in priporočili omejuje nedopustno poseganje oblasti v človekove pravice in temeljne svoboščine. Nanj se lahko obrne vsakdo, ki meni, da je državni organ, organ lokalne skupnosti ali nosilec javnih pooblastil kršil njegove pravice ali temeljne svoboščine. Varuhove pristojnosti so omejene na nadzorovanje javne oblasti, zato ne more preiskovati kršitev, ki jih povzročijo osebe zasebnega prava,

[19] ang. Public sector information.

lahko pa predlaga informacijskemu pooblaščencu, da opravi nadzor in sprejme ustrezne ukrepe.

Institucija varuha človekovih pravic je bila v slovenski ustavni sistem vpeljana z Ustavo Republike Slovenije, sprejeto leta 1991. Varuha opredeljuje 159. člen, ki določa, da se za varovanje človekovih pravic in temeljnih svoboščin v razmerju do državnih organov, organov lokalne samouprave in nosilcev javnih pooblastil z zakonom določi varuha pravic državljanov. V drugem odstavku pa je določeno, da se z zakonom za posamezna področja določijo posebni varuhi pravic. Zakonodajalec je to možnost izkoristil nekoliko drugače, kajti za področje varstva osebnih podatkov ni določil posebnega varuha človekovih pravic, pač pa je z ZVOP-1 varuhu podelil posebno pristojnost neodvisnega nadzora nad varstvom osebnih podatkov.

Leta 1993 je Državni zbor RS sprejel Zakon o varuhu človekovih pravic[20], ki določa njegova pooblastila ter daje zakonsko podlago za njegovo ustanovitev. V skladu z ZVČP traja mandat varuha šest let, z možnostjo ponovne izvolitve za eno mandatno obdobje. Varuh ima najmanj dva in največ štiri namestnike, ki jih na varuhov predlog prav tako za šest let imenuje Državni zbor RS. Namestniki imajo na področjih, za katera so pristojni, vsa pooblastila, ki jih zakon daje varuhu. S tem ko varuh za izvajanje nalog na posameznem področju določi enega od namestnikov, je dosežena določena individualizacija opravljanja te naloge, hkrati pa se ne posega v notranjo organizacijo in delitev dela pri varuhu.

Varuh je uradno začel z delom leta 1995. S tem je tudi nehal delovati Svet za varstvo človekovih pravic.

S spremembami in dopolnitvami ZVOP-1 v letu 2001 je Varuh dobil novo zadolžitev. Zakon namreč v četrtem poglavju četrtega dela določa, da Varuh neposredno nadzoruje spoštovanje predpisov o varstvu osebnih podatkov pri upravljavcu zbirk in pri uporabnikih osebnih podatkov, spremlja oziroma nadzira delo Inšpektorata za varstvo osebnih podatkov, svetuje v zadevah na tem področju, sodeluje v postopkih sprejemanja predpisov in opravlja druge naloge na podlagi zakona.
Zakon določa tudi, da varuh v letnem poročilu poroča Državnemu zboru RS o ugotovitvah, predlogih in priporočilih ter o stanju na področju varstva osebnih podatkov.

[20] ZVČP, UL RS, št. 71/93.

6 VARSTVO OSEBNIH PODATKOV V POLICIJI

6.1 ZAKON O POLICIJI

V četrto poglavje Zakona o policiji[21], »Zbiranje, varstvo in zavarovanje podatkov«, spadajo členi od 54. od 64. Policisti svoje podatke sicer pridobivajo posredno in neposredno. Neposredno pridobivanje podatkov določa 33. člen ZPol, ki pravi da smejo policisti pri opravljanju svojih nalog opozarjati, ukazovati, ugotavljati identiteto in izvesti identifikacijski postopek, opraviti prepoznavo po fotografijah, varnostno preverjati osebe, izvajati prikrito evidentiranje ali namensko kontrolo, vabiti, opraviti varnostni pregled, prepovedati gibanje, prepovedati približevanje določeni osebi, kraju ali območju, opraviti protiteroristični pregled prostorov, objektov, naprav in območij, prijeti in privesti osebo, pridržati osebo, odrediti strožji policijski nadzor, zaseči predmete, vstopiti v tuje stanovanje in tuje prostore, uporabiti prevozna in komunikacijska sredstva, uporabiti prisilna sredstva ter porabiti druga pooblastila, določena v zakonih. Posredno policisti podatke pridobivajo iz uradnih evidenc, preko centralnega računalnika.
Zpol določa, da policija sme, če je to potrebno zaradi opravljanja z zakonom določenih nalog policije, organom tujih držav ali mednarodnih organizacij, na njihovo zaprosilo ali lastno pobudo, ob pogoju dejanske vzajemnosti, posredovati zbrane osebne in druge podatke. Pred posredovanjem teh podatkov policija pridobi zagotovila, da ima država, v katero se podatki iznašajo, urejeno varstvo osebnih podatkov in da bo organ tuje države ali mednarodne organizacije uporabil osebne podatke samo za namene, določene s tem zakonom. Jasno je tudi določeno, da se za zbiranje, obdelovanje, shranjevanje, posredovanje in uporabo podatkov policijskih evidenc uporabljajo določbe Zakona o varstvu osebnih podatkov.

Policija upravlja zbirke osebnih podatkov, ki jih zaradi opravljanja nalog zbirajo, obdelujejo, shranjujejo, posredujejo in uporabljajo policisti. V zvezi z izvajanjem policijskih pooblastil Policija vodi in vzdržuje evidence, ki so naštete v 59. členu ZPol:

- evidenco kaznivih dejanj;
- evidenco kršiteljev in prekrškov;
- evidenco iskanih oseb;
- evidenco identifikacij;
- evidenco operativnih informacij;
- evidenco oseb, zoper katere so bili izvedeni prikriti preiskovalni ukrepi iz zakona, ki ureja kazenski postopek;
- evidenco DNK-preiskav;
- evidenco dogodkov;
- evidenco pridržanih in zadržanih oseb;

[21] ZPol-UPB6, UL RS št. 107/06

- evidenco varnostno preverjenih oseb;
- evidenco pritožb;
- evidenco uporabe prisilnih sredstev;
- evidenco daktiloskopiranih oseb;
- evidenco fotografiranih oseb;
- evidenco iskanih in najdenih predmetov;
- evidenco usmerjenega zbiranja obvestil na področju terorizma in mednarodnega organiziranega kriminala;
- evidenco vstopov in gibanja oseb v varovanih objektih Policije in na območju okolišev teh objektov;
- evidenco izdanih odredb za prepoved približevanja;
- evidenco prikritih evidentiranj in namenskih kontrol.

Te evidence vsebujejo naslednje skupne osebne podatke:

- osebno ime,
- rojstne podatke,
- EMŠO,
- spol,
- naslov stalnega oz. začasnega prebivališča,
- državljanstvo.

6.2 PRAVILNIK O VAROVANJU PODATKOV POLICIJE

Na podlagi 16. člena Zakona o državni upravi[22] in 57. člena Zakona o policiji je bil dne, 31. 05. 2008, izdan nov Pravilnik o varovanju podatkov Policije, ki je nadomestil prejšnjega, sprejetega leta 1999.

Ta pravilnik določa organizacijske in logično-tehnične postopke ter ukrepe za varovanje podatkov Policije. S tem zagotavlja varno obravnavanje osebnih podatkov, omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki obravnavani in kdo jih je obravnaval, in sicer za obdobje, za katero se podatki hranijo.

V pravilniku so razloženi nekateri izrazi, ki niso razloženi na začetku te naloge:

- varovani podatek: osebni ali drug podatek, ki ni tajni podatek, njegovo razkritje nepoklicanim osebam pa bi povzročilo škodo organu, poteku uradnih postopkov ali osebam, na katere se nanaša, zato mora njegovo obravnavanje spremljati izvajanje določenih varnostnih ukrepov;

[22] Zdu-1, UL RS, št. 113/05.

- obravnavanje podatkov: postopki in procesi zbiranja, obdelave, hrambe, posredovanja, uporabe in uničenja podatkov;

- računalniško obravnavanje podatkov: obravnavanje podatkov s pomočjo računalnika in z napravami, ki rabijo pomnilnik za shranjevanje celega ali dela računalniškega programa in vseh ali dela podatkov, ki so potrebni za izvajanje tega programa;

- informacijski in telekomunikacijski sistem Policije (ITSP): urejena celota podatkov in informacij, metod in sredstev za neposredno opravljanje informacijske dejavnosti ter telekomunikacijska infrastruktura, ki se kot zaprt uporabniški sistem uporablja za obravnavo nalog Policije;

- lokalni informacijski sistem (v nadaljnjem besedilu: LIS): urejena celota podatkov in informacij, metod in sredstev za neposredno opravljanje informacijske dejavnosti, s pomočjo katere organizacijske enote Policije na eni ali več delovnih postajah ali strežnikih obravnavajo podatke;

- vodja LIS: delavec Policije, ki je odgovoren za obravnavanje podatkov v okviru LIS. Vodjo LIS določi vodja enote[23].

Delavec Policije ob sklenitvi delovnega razmerja ali premestitvi na delovno mesto, na katerem bo obravnaval varovane podatke, s pisno izjavo[24] potrdi, da je seznanjen s predpisi, ki v Policiji urejajo varstvo zaupnih in osebnih podatkov ter varovanje teh podatkov. Delavec Policije lahko varovane podatke uporablja le za opravljanje z zakonom določenih nalog in skladno z navodili, ki urejajo način obravnavanja posameznih podatkov. Peti člen pravilnika določa, da z vsebino varovanih podatkov delavec Policije, ki te podatke obravnava, ne sme seznaniti drugih oseb. Kadar opravljanje nalog Policije zahteva, da se z določenimi varovanimi podatki seznanijo tudi druge osebe, mora delavec Policije pred posredovanjem teh podatkov dobiti predstojnikovo dovoljenje, razen kadar gre za delavce Policije ali ministrstva, pristojne za izvajanje nadzora nad opravljanjem nalog Policije.

Če pa je v obravnavanje podatkov ali v izgradnjo oziroma vzdrževanje infrastrukture ITSP vključen zunanji izvajalec, mora biti dolžnost varovanja osebnih ali tajnih podatkov, katere upravlja Policija, vključena v pogodbo, s katero se uredijo razmerja in odnosi med Policijo in izvajalcem pogodbenih del. Izvajalčev delavec mora s pisno izjavo[25] potrditi, da je seznanjen z dolžnostjo varovanja tajnih ali osebnih podatkov Policije, ki jih bo obravnaval pri izvajanju pogodbenih del.

Pravilnik določa splošne varnostne ukrepe, ki so jih delavci Policije dolžni izvajati zaradi varovanja podatkov:

[23] Glej Priloga št. 1.
[24] Glej Priloga št. 2.
[25] Glej Priloga št. 3.

- kadar zapuščajo svoje delovne prostore, morajo zakleniti pisalne mize, omare, blagajne in pisarne, v katerih hranijo varovane podatke;
- dokumentov ali medijev z varovanimi podatki ne smejo puščati na odprtih površinah pisarniške opreme ali drugih mestih, kjer so dostopne nepoklicanim osebam;
- navodila za uporabo računalniško vodenih evidenc morajo hraniti tako, da niso dostopna nepoklicanim osebam;
- dosledno morajo izvajati postopek prijave oziroma odjave s svojim osebnim geslom na začetku oziroma ob zaključku dostopa do varovanih podatkov, shranjenih v evidencah ITSP;
- po končani izdelavi dokumentov z varovanimi podatki morajo poskrbeti za uničenje pomožnega gradiva;
- upoštevati morajo druge predpise, ki jih zavezujejo, kako naj pri svojem delu ravnajo z varovanimi podatki.

V osmem poglavju je opredeljena obveza fizičnega in tehničnega varovanja prostorov, v katerih se obravnavajo varovani podatki.

Poleg hišnega reda so za gibanje v teh prostorih in objektih določena še naslednja pravila:

- zadrževanje delavcev v teh prostorih, razen tistih, ki so v njem zaposleni ali je njihova prisotnost nujno potrebna za nemoteno opravljanje delovnih nalog, ni dovoljeno;
- obiski zunanjih strank so dovoljeni samo z odobritvijo vodje enote in v spremstvu najmanj enega delavca Policije;
- obiski serviserjev informacijske ali telekomunikacijske opreme so dovoljeni smo na poziv vzdrževalne službe ITSP, serviserja pa mora med obiskom nadzorovati vodja LIS oziroma delavec vzdrževalne službe ITSP.

Poleg standardnih varnostnih ukrepov, ki jih za objekte Policije predpisuje akt o varstvu pred požarom, velja za prostore, v katerih je instalirana programska oprema, še naslednje:

- prepoved uporabe odprtega ognja;

- prepoved nameščanja začasne električne napeljave;
- hramba gorljivih snovi samo v količinah, ki so nujno potrebne za nemoten potek dela;
- ognjevarne omare, v katerih so shranjeni mediji, morajo biti vedno zaprte.

Pravilnik opredeljuje varovanje strojne opreme. Strojno opremo ITSP je dovoljeno uporabljati le za izvajanje nalog Policije, uporablja pa jo lahko le ustrezno usposobljen delavec Policije. Poleg neposrednih uporabnikov imajo dostop do strojne opreme ITSP še delavci Policije, ki jo vzdržujejo in pogodbeno vezani zunanji vzdrževalci.

Urad za informatiko in telekomunikacije Policije (urad) mora vsem LIS zagotoviti pisna navodila o načinu uporabe strojne in programske opreme ter o ukrepih v primeru izpada ali okvare.

V Policiji se za obravnavanje podatkov lahko uporablja le sistemizirana računalniška programska oprema (programi), ki je predpisana s sistematizacijo tehnične opreme in skladna s standardi ITSP. Program lahko samoiniciativno izdela tudi delavec Policije, pred vključitvijo v uporabo pa mora biti atestiran. To opravi urad, ki nato organizira tudi njegovo namestitev. Urad določa tudi avtorizacijo za brisanje, kopiranje in spreminjanje programa ter kje se hrani kopija le-tega.

Programi, ki jih za potrebe ITSP Policija kupi od proizvajalcev programske opreme, mora biti opremljen z licenco, ki Policiji dovoljuje namestitev in uporabo programov na načrtovanem številu lokacij v organizacijskih enotah Policije.

Dostop do varovanih podatkov mora biti varovan s sistemom, ki preveri identiteto uporabnika in njegovo upravičenost za dostop do podatkov in drugih virov ITSP. Sistem mora onemogočati lažno predstavitev identitete ali upravičenosti oz. dostop do podatkov drugih virov ITSP v imenu drugega uporabnika, ne da bi ta za to vedel.

Zapis sistema kontrole in evidentiranja mora omogočati naknadno ugotavljanje, kateri uporabnik je v določenem času z določenega terminala, delovne postaje ali drugega sredstva obravnaval varovane podatke, in sicer za obdobje, za katero se posamezni podatki hranijo. Rok hrambe zapisa dostopov je enak roku hrambe podatkov v varovanih evidencah. Uporabniki morajo biti seznanjeni z vrsto zapisov v dnevnik dela in časom hrambe.

Z dnevnikom upravlja Generalna policijska uprava oz. njena enota, pristojna za zaščito podatkov. Ta enota lahko na podlagi pisnega zahtevka generalnega direktorja Policije ali organizacijske enote Generalne policijske uprave, pristojne za notranje

preiskave, iz dnevnika dela izpiše podatke, potrebne za preverjanje upravičenosti obravnavanja varovanih podatkov.

Osmo poglavje obravnava varovanje podatkov in medijev:

- terminali v prostorih, namenjenih stikom z zunanjimi obiskovalci, morajo imeti zaslone obrnjene tako, da je nepoklicanim pogled onemogočen;
- za vse varovane podatke in vso programsko opremo na glavnem računalniku mora urad imeti kopijo in dvojnik kopije. Dvojnik kopije mora biti shranjen na varovani lokaciji izven objekta;
- kopijo podatkov, ki se obdelujejo lokalno, ter kopijo sistemskih nastavitev lokalnih strežnikov, vodi vodja LIS;
- roke, način dopolnjevanja in medije za hranjenje določi Urad za vsako evidenco posebej.

Delavec Policije, ki ugotovi, da se je nepoklicana oseba seznanila z varovanimi podatki, je to dolžan nemudoma sporočiti vodja enote, ta pa enoti Generalne policijske uprave, pristojni za zaščito podatkov in organizacijski enoti, pristojni za notranjo varnost. Če delavec dokument ali medij z varovanimi podatki izgubi ali pogreši, mora o tem takoj obvestiti vodjo enote, sam pa ukreniti vse potrebno, da se ugotovijo okoliščine, v katerih je medij izginil, odstranijo škodljive posledice in zavarujejo sledi.

Dostop do drugih informacijskih sistemov in interneta ima lahko le delavec Policije, ki potrebuje podatke ali druge storitve teh sistemov za opravljanje delovnih nalog in ima tak priključek določen v tehnični sistematizaciji.

ITSP je z drugimi informacijskimi sistemi in internetom lahko povezan le na način, ki nepooblaščenim uporabnikom preprečuje dostop do varovanih podatkov in naprav, s katerimi se varovani podatki obravnavajo. Dostop poteka preko skupnih, ustrezno varovanih priključnih točk ITSP. Na priključni točki mora biti nameščena varnostna pregrada, ki mora omogočati:

- upravljanje dostopa delavcev Policije do drugih informacijskih sistemov in interneta;
- upravljanje dostopa uporabnikov drugih informacijskih sistemov do varovanih podatkov in naprav, s katerimi se ti podatki obravnavajo;
- zaznavanje in preprečevanje poskusov vdorov v ITSP;
- preprečevanje in odkrivanje poskusov vnosov računalniških virusov;

- kriptozaščito prenosov varovanih podatkov Policije preko infrastrukture drugega informacijskega sistema ali interneta.

Na predlog predstojnika enote se lahko zaradi nemotenega izvajanja nalog Policije v enoto namesti delovna postaja, ki je na internet priključena mimo varnostne pregrade, ne sme pa biti povezana z omrežjem ITSP. Na njej prav tako ne smejo biti shranjeni varovani podatki Policije.

Če je na varnostni pregradi nameščen sistem, ki omogoča spremljanje aktivnosti posameznega delavca Policije, mora biti o tem na nedvoumen in jasen način opozorjen. Varnostna pregrada mora na spremljanje in evidentiranje dostopov opozoriti tudi zunanje uporabnike interneta in drugih informacijskih sistemov, preden se povežejo z viri ITSP.

Nadalje so v Pravilniku določeni še ukrepi in postopki za varovanje prenosa podatkov po telekomunikacijskih zvezah ali v fizični obliki, po pošti. Prav tako je določena odgovornost vodij enote za izvajanje ukrepov in postopkov varovanja podatkov ter nadzor nad izvajanjem teh ukrepov.

6.3 KATALOG ZBIRK OSEBNIH PODATKOV V POLICIJI

Kot je bilo omenjeno ob razlagi Zakona o varovanju osebnih podatkov, mora upravljalec podatkov za vsako zbirko osebnih podatkov, ki jo vodi, vzpostaviti katalog. V oktobru 2007 je bila tako izdana zadnja verzija Kataloga zbirk osebnih podatkov v Policiji, ki vsebuje vseh 33 evidenc osebnih podatkov, ki jih Policija vodi. Poleg evidenc iz 59. člena ZPol so to še :

- Evidenca o vizumih, izdanih tujcem;
- Evidenca o nastanitvah tujcev v centru za tujce;
- Evidenca izrečenih kazni izgona tujca iz države;
- Evidenca varstvenih ukrepov odstranitve tujca iz države;
- Evidenca tujcev, ki jim je odrejen strožji policijski nadzor;
- Evidenca tujcev, ki jim je odrejeno bivanje izven centra za tujce;
- Evidenca o tujcih, ki im je bil zavrnjen vstop v državo;
- Evidenca o prisilno odstranjenih tujcih;
- Evidenca policijske prijave;
- Evidenca dovoljenj za obravnavo tajnih podatkov;
- Evidenca oseb, za katere se izvede postopek ugotavljanja identitete po 35. čl. ZNDM;
- Evidenca izdanih certifikatov o usposobljenosti voznikov vozil za prevoz nevarnega blaga v cestnem prometu;

- Evidenca pravnih oseb in samostojnih podjetnikov, ki so imenovali varnostnega svetovalca.

Vsaka evidenca v skladu z ZVOP-1 vsebuje:

- naziv zbirke;
- podatke o upravljavcu;
- pravno podlago za obdelavo osebnih podatkov;
- kategorije posameznikov, na katere se nanašajo osebni podatki;
- vrste osebnih podatkov v zbirki osebnih podatkov;
- namen obdelave;
- rok hrambe osebnih podatkov;
- omejitev pravic posameznikov glede osebnih podatkov v zbirki osebnih podatkov in pravno podlago za omejitev;
- uporabnike ali kategorije uporabnikov osebnih podatkov, vsebovanih v zbirki osebnih podatkov;
- dejstvo, ali se osebni podatki iznašajo v tretjo državo, kam, komu in pravno podlago iznosa;
- splošni opis zavarovanja osebnih podatkov;
- podatke o povezanih zbirkah osebnih podatkov iz uradnih evidenc ter javnih knjig;
- podatke o zastopniku iz tretjega odstavka 5. člena ZVOP-1.

PRIMER:

EVIDENCA KAZNIVIH DEJANJ

1. NAZIV ZBIRKE OSEBNIH PODATKOV
Evidenca kaznivih dejanj

2. PODATKI O UPRAVLJAVCU OSEBNIH PODATKOV (ZA PRAVNO OSEBO: NAZIV OZIROMA FIRMO IN NASLOV OZIROMA SEDEŽ UPRAVLJAVCA OSEBNIH PODATKOV IN MATIČNO ŠTEVILKO)
MNZ Policija
Štefanova ulica 2, Ljubljana
Matična številka: 1332813000

3. PRAVNA PODLAGA ZA OBDELAVO OSEBNIH PODATKOV
Zakon o policiji
Zakon o kazenskem postopku

4. KATEGORIJE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI
- ovadene osebe

- osumljenci
- oškodovanci
- prijavitelji
- druge osebe, ki so dale informacije o kaznivem dejanju

5. VRSTE OSEBNIH PODATKOV V ZBIRKI OSEBNIH PODATKOV
- osebno ime,
- rojstni podatki (dan, mesec, leto, kraj),
- EMŠO,
- spol,
- naslov stalnega oziroma začasnega prebivališča,
- državljanstvo,
- vzdevek ali lažno ime,
- osebni opis,
- narodnost ovadene osebe ali osumljenca,
- upravna enota kraja rojstva,
- njene družinske in premoženjske razmere,
- šolska izobrazba,
- poklic in zaposlitev,
- osebni podatki oškodovancev, prijaviteljev in drugih oseb, ki so dale obvestila o kaznivem dejanju,
- podatki o kaznivem dejanju (vrsta, kraj, čas, način, motiv, opis predmetov kaznivega dejanja, škoda in druge okoliščine izvršitve).

6. NAMEN OBDELAVE
- preprečevanje, odkrivanje in preiskovanje kaznivih dejanj;
- odkrivanje in prijemanje storilcev kaznivih dejanj;
- dokumentiranje dela policije v predkazenskem in kazenskem postopku;
- preventivno delovanje Policije;
- načrtovanje dela Policije;
- poročanje o stanju kriminalitete v RS, analiziranje podatkov o kriminaliteti;
- zagotavljanje podatkov pravosodnim organom in drugim organom in organizacijam.

7. ROK HRAMBE OSEBNIH PODATKOV
- do ustavitve policijske preiskave oziroma zaključka akcije varovanja;
- do pravnomočne odločitve o uvedbi kazenskega postopka oziroma postopka o prekršku;
- če te ni, pa do zastaranja pregona.
Državno tožilstvo, ki prejme kazensko ovadbo Policije, je dolžno odstopiti pristojni policijski enoti odločbo o pravnomočni uvedbi kazenskega postopka, na podlagi katere Policija določa roke hrambe v evidenci kaznivih dejanj.

8. OMEJITVE PRAVIC POSAMEZNIKOV GLEDE OSEBNIH PODATKOV V ZBIRKI OSEBNIH PODATKOV IN PRAVNA PODLAGA OMEJITEV
Posameznik ima pravico vpogleda v svoje podatke po pravnomočni odločitvi o uvedbi kazenskega postopka ali postopka o prekršku; če ta ni uveden, pa po zastaranju

pregona. Če so podatki zbrani brez njegove vednosti in niso bili izbrisani, se o tem obvesti, ko to dopušča narava policijskega dela.

9. UPORABNIKI ALI KATEGORIJE UPORABNIKOV OSEBNIH PODATKOV, VSEBOVANIH V ZBIRKI OSEBNIH PODATKOV

KRIM, PN

Komentar [g1]: Kaj je to?

- policija,
- državna tožilstva,
- sodišča,
- centri za socialno delo – mladoletniki,
- razni drugi državni organi (MZZ, SOVA, Urad za preprečevanje pranja denarja, MORS, ...),
- Slovensko zavarovalno združenje in slovenske zavarovalnice,
- udeleženci v prometnih nesrečah.

10. ALI SE OSEBNI PODATKI IZNAŠAJO V TRETJO DRŽAVO, KAM, KOMU IN PRAVNA PODLAGA IZNOSA
- Interpol,
- policijam drugih držav, s katerimi ima R Slovenija podpisane mednarodne pogodbe;
- Zakon o policiji,
- Zakon o kazenskem postopku,
- mednarodne pogodbe.

11. SPLOŠEN OPIS ZAVAROVANJA OSEBNIH PODATKOV
- vsi dostopi do osebnih podatkov, ki se obdelujejo v okviru informacijskega sistema policije, so varovani s fizičnimi, tehničnimi in organizacijskimi ukrepi;
- prijava oziroma odjava z osebnim geslom (posebno ščitenje tajnih podatkov);
- sistem kontrole in evidentiranja dostopa do podatkov;
- kriptografska zaščita podatkov, ki se posredujejo z računalniško izmenjavo podatkov.

12. PODATKI O POVEZANIH ZBIRKAH OSEBNIH PODATKOV IZ URADNIH EVIDENC TER JAVNIH KNJIG

13. PODATKI O ZASTOPNIKU IZ TRETJEGA ODSTAVKA 5. ČLENA ZVOP1

6.4 DRUGI PREDPISI

Poleg omenjenih sta v Policiji v uporabi še dva pomembnejša predpisa, in sicer Pravilnik o načinu vodenja policijskih evidenc in Pravilnik o hrambi podatkov o elektronskih komunikacijah Policije in o dostopu do policijskih zbirk podatkov.

Pravilnik o načinu vodenja policijskih evidenc ureja način vodenja evidenc, kar zajema tudi vzdrževanje evidenc, hranjenje podatkov evidenc in virov, iz katerih so bili podatki vneseni v evidence, ter posredovanje podatkov iz evidenc in uveljavljanje pravic posameznika. V okviru tega pravilnika je pomembno četrto poglavje, ki govori o posredovanju osebnih podatkov.

Podatki se posredujejo:

- posameznikom, ki so do posredovanja upravičeni na osnovi zakona in izkazanega pravnega interesa;
- pravnim osebam, skladno z zakonom.

S Pravilnikom o hrambi podatkov o elektronskih komunikacijah Policije in o dostopu do policijskih zbirk podatkov se ureja hramba podatkov, ki se obdelujejo zaradi telefonskih in radijskih komunikacij v informacijsko telekomunikacijskem sistemu Policije, o izmenjavi sporočil interne elektronske pošte Policije, o uporabi interneta uporabnikov, registriranih v domeni policija.si, ter hramba podatkov o dostopu do podatkov policijskih evidenc in drugih zbirk podatkov Policije. Ta pravilnik ureja tudi snemanje klicev na telefonsko številko 113 in govornih radijskih komunikacij ITSP ter snemanje vsebine drugih komunikacij, ki jih na podlagi tega pravilnika s pisno odredbo določi generalni direktor Policije. Shranjeni podatki in posnetki se uporabljajo za identificiranje, registriranje in reševanje klicev v sili, ki jih prejme Policija, ter da se policiji, organom, pristojnim za nadzor nad njenim delovanjem, in drugim organom, pooblaščenim z zakonom, omogoči rekonstrukcija ter preverjanje zakonitosti in strokovnosti postopkov in ukrepov, ki jih je v zvezi s posamezno nalogo izvedla Policija.

6.5 SCHENGENSKI INFORMACIJSKI SISTEM IN VARSTVO PODATKOV

Schengenski sporazum z dne, 14. junija 1985, in Konvencija o izvajanju Schengenskega sporazuma z dne, 19. junija 1990, (Schengenska konvencija) sta odpravila mejne kontrole na notranjih mejah med državami pogodbenicami (poleg držav članic EU, razen Velike Britanije in Irske, tudi Norveška in Islandija). S tem se je ustvaril skupni prostor za prost pretok oseb in za pospešitev prevoza in pretoka blaga ter uveljavilo načelo mejne kontrole ob vstopu v enotno Schengensko območje. Zato je bilo za ohranjanje zadovoljive ravni javnega reda in javne varnosti, vključno z nacionalno varnostjo, med drugimi ukrepi (krepitev policijskega in pravosodnega

sodelovanja, harmonizacija vizne in azilne politike) potrebno tudi oblikovanje Schengenskega informacijskega sistema (SIS).

SIS obsega nacionalne podatkovne zbirke v vsaki državi pogodbenici in tehnični podporni del v Strassbourgu. Za namene mejnih in drugih policijskih kontrol, tudi tistih, ki se izvajajo v notranjosti države, tehnični podporni del s prenosom informacij *on-line* zagotavlja, da nacionalne podatkovne zbirke vsebujejo enake podatke. Pri tem vsebuje SIS le in samo točno določene kategorije podatkov, ki jih vnašajo preko nacionalne podatkovne zbirke le države pogodbenice, če so podatki dovolj pomembni za vnos v SIS in so v skladu s predhodno opisanim namenom. Zato vsaka pogodbenica imenuje organ z osrednjo odgovornostjo za njen nacionalni del SIS, ki se imenuje SIRENE – Supplementary Information Request at the National Entry, v Sloveniji je ta organ vzpostavljen v okviru Policije.
Ta skupni sistem omogoča povezavo med državami pogodbenicami in omogoča končnim uporabnikom (policija, carina, konzulati in druge službe, pristojne za obdelavo podatkov v zvezi z vizumi, za izvajanje zakonodaje o tujcih ali za izdajo potrdil o registraciji vozil) dostop do informacij, ki so jih vnesle v SIS druge države pogodbenice in ki jih potrebujejo za opravljanje svojih dolžnosti.
Zbirka podatkov, ki si jo tako delijo vse države na Schengenskem območju, vsebuje dve široki kategoriji podatkov:

- podatke o iskanih ali pogrešanih osebah in osebah, ki se jim tajno sledi (prikrito evidentiranje);
- podatke o ukradenih ali drugače odtujenih vozilih in drugih predmetih (osebni dokumenti, orožje in denar).

V SIS se hranijo podatki o:

- osebah, za katere se zahteva prijetje zaradi predaje ali izročitve (95. člen Schengenske konvencije);
- osebah, ki niso državljani držav članic, za katere je razpisana zavrnitev vstopa v Schengensko območje (96. člen Schengenske konvencije);
- pogrešanih osebah ali osebah, ki potrebujejo začasno policijsko zaščito, predvsem mladoletni (97. člen Schengenske konvencije);
- pričah oziroma osebah, ki se morajo v okviru kazenskega postopka zglasiti na sodišču ali jim je potrebno vročiti sodbo ali vabilo na prestajanje kazni (98. člen Schengenske konvencije), in osebah za namene prikritega evidentiranja ali namenske kontrole (99. člen Schengenske konvencije).

Pri tem so lahko za osebe zabeleženi samo naslednji podatki:

- priimek in ime, morebitni psevdonim, po potrebi v novem podatkovnem zapisu;
- morebitne objektivne fizične posebnosti, ki se ne spreminjajo;
- prva črka drugega imena;
- datum in kraj rojstva;

- spol;
- državljanstvo;
- ali so te osebe oborožene;
- ali so te osebe nasilne;
- razlog za razpis ukrepa;
- predlagana oblika ukrepanja.

Podatki so skrbno varovani, zanje se v okviru SIS poleg določil Schengenske konvencije in Zakona o varstvu osebnih podatkov upošteva tudi določila že omenjene Konvencije Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov.

V SIS vnašajo podatke vse države pogodbenice, dostop do tega sistema pa morajo imeti tako Policija pri mejni kontroli na zunanji meji, kot tudi drugi državni organi, ki so za to pooblaščeni v skladu s Schengensko konvencijo (npr. veleposlaništva pri izdaji vizumov, upravne enote pri izdajanju dovoljenj za prebivanje za tujce).

Tako imajo pravico dostopa do podatkov, ki so shranjeni v SIS, izključno službe, ki so pristojne za:
- mejno kontrolo;
- konkretno določena policijska in carinska preverjanja v notranjosti države ter za njihovo koordinacijo;
- v določeni meri tudi pravosodni organi v zvezi s kazenskimi postopki (npr. tožilstvo).

V podatke v zvezi z zavrnitvijo vstopa tujcu po 96. členu in v zvezi z osebnimi dokumenti iz člena 100 (točki d in e 3. odstavka) Schengenske konvencije, ki so bili ukradeni, protipravno odvzeti ali drugače odtujeni (potni listi, osebne izkaznice, vozniška dovoljenja), imajo vpogled še:
- službe, pristojne za dodeljevanje vizumov;
- centralni organi, pristojni za obdelavo prošenj za vizum;
- službe, pristojne za dodeljevanje dokumentov o bivanju;
- službe, pristojne za izvajanje predpisov s področja tujcev.

Nadalje imajo pravico dostopa do podatkov o ukradenih, protipravno odtujenih ali izgubljenih vozilih (točki a in b 3. odstavka 100. člena Schengenske konvencije) in podatkov o ukradenih, protipravno odtujenih, izgubljenih ali preklicanih prometnih dovoljenjih in registrskih tablicah vozil tudi vladne in druge službe, ki so v državah članicah EU odgovorne za izdajanje potrdil o registraciji vozil iz Direktive Sveta 1999/37/ES z dne, 29. aprila 1999, o dokumentih za registracijo vozil.

Seznam organov, ki so pristojni dostopati do podatkov, vsebovanih v SIS, določi država pogodbenica in njihov seznam posreduje Izvršnemu odboru, ki je bil ustanovljen za namene izvajanja Schengenske konvencije.

6.5.1 Zavarovanje in nadzor nad varstvom osebnih podatkov v SIS

Tehnični podporni del sistema je v Strassbourgu in s prenosom informacij *on-line* zagotavlja, da nacionalne podatkovne zbirke držav podpisnic vsebujejo enake podatke. Temelj SIS je tako posebej varovana linija, ki kot vodnik omogoča pretok informacij, ki so zakodirane. To so močno varovane linije. Podatkovne baze so zaščitene, vsaka država pa ima svojo nacionalno kopijo.

Za nadzor nad izvajanjem tehničnega podpornega dela SIS je glede varstva osebnih podatkov pristojen Skupni nadzorni organ, za nadzor nacionalne podatkovne zbirke pa nacionalni nadzorni organ vsake pogodbenice, v Sloveniji je to Informacijski pooblaščenec. Ta je pristojen za izvajanje neodvisnega nadzora podatkovnih zbirk nacionalnega dela SIS in za preverjanje, da obdelava in uporaba podatkov, vnesenih v SIS, ne pomeni kršenja pravic oseb, na katere se podatki nanašajo.

Skupni nadzorni organ je neodvisni organ za nadzor tehničnega podpornega dela SIS in je ustanovljen na podlagi 115. člena Schengenske konvencije.

Ta organ sestavljata po dva predstavnika vsakega nacionalnega nadzornega organa. Vsaka pogodbenica ima en glas.

7 PRIMERI IZ PRAKSE

7.1 NEUPRAVIČENO POSREDOVANJE PODATKOV LOVSKI DRUŽINI

PRITOŽBENI RAZLOGI
Občan je podal pritožbo zoper ravnanje policistov Policijske postaje in pobudo Varuhu človekovih pravic, saj so policisti po njegovem prepričanju neupravičeno posredovali podatke o postopku z njim in o obravnavanem kaznivem dejanju lovski družini, katere član je.

UGOTOVITVE
V postopku preverjanja pritožnikovih oziroma pobudnikovih navedb je bilo ugotovljeno, da je lovska družina pisno zaprosila Policijsko postajo za določene podatke o svojem članu, ki naj bi mu policisti zasegli orožje. Policijska postaja je prosilcu posredovala pisni odgovor, v katerem je navedla osebne podatke pritožnika, podatke o postopku z njim, podatke o orožju, ki mu je bilo zaseženo, katerega kaznivega dejanja je osumljen ter kakšen ukrep bo izveden zoper njega.

UKREPI
Na pisno zaprosilo Varuha človekovih pravic, da vodstvo Policijske postaje pojasni razloge za svoje ravnanje, je to sporočilo, da je bil odgovor lovski družini poslan v skladu z Uredbo o upravnem poslovanju[26]. S pojasnili se Varuh človekovih pravic ni strinjal ter s svojim mnenjem glede kršenja pravic pobudniku med drugim seznanil tudi Informacijskega pooblaščenca. Državna nadzornika za varstvo osebnih podatkov pri omenjeni instituciji sta izvedla inšpekcijski nadzor na navedeni policijski postaji in pri tem ugotovila kršitev določil Zakona o varstvu osebnih podatkov. Komandirju policijske postaje je bilo v zvezi s tem izrečeno opozorilo.
Tudi člani Senata za reševanje pritožb Policije so bili soglasni, da je pritožba zoper ravnanje policistov utemeljena.

MNENJE
V omenjenem primeru je bilo ravnanje odgovornih na Policijski postaji v nasprotju z veljavnimi predpisi, saj v konkretnem primeru ni bilo nikakršne zakonite podlage za posredovanje vsebinsko tako obširnega odgovora lovski družini. Vsebina odgovora je presegla okvire dovoljenih informacij in podatkov, do katerih so upravičeni tisti, ki naslavljajo vloge oziroma dopise v skladu z Uredbo o upravnem poslovanju. Ta sicer

[26] Uredba o upravnem poslovanju (Ur. list. RS, št. 20/05, 106/05, 30/06, 86/06 in 63/07)
18. člen (Odgovarjanje na prejete dopise):
Organ mora odgovoriti na vse dopise, ki jih prejme v fizični ali elektronski obliki, razen če so šikanoznega značaja. Organ mora na dopis odgovoriti najkasneje v 15 dneh po prejemu le-tega, če je iz dopisa razviden naslov pošiljatelja. Za zahtevnejše zadeve mora organ v tem roku izdati vsaj obvestilo o nadaljnjem ukrepanju/postopanju in realnem roku. Organ mora odgovarjati tudi na dopise v elektronski obliki, ki so prejeti preko enotnega državnega portala.

res nalaga organom, da morajo odgovoriti na vse dopise, ki jih prejmejo v fizični obliki, razen če so šikanoznega značaja. Vendar pa morajo odgovorni pri sestavljanju odgovorov paziti, do kakšnih podatkov je prosilec upravičen, in temu primerno prilagoditi vsebino. V tem primeru je odgovor namreč vseboval osebne podatke ovadene osebe, kvalifikacijo kaznivega dejanja, ki ga je oseba osumljena, ter druge okoliščine in podatke o izvedenih ukrepih v zvezi z obravnavanim kaznivim dejanjem, do katerih pa lovska družina ni upravičena. S tem pa so bila kršena tudi določila Zakona o varstvu osebnih podatkov. Osmi člen ZVOP-1 namreč določa, da se osebni podatki lahko »obdelujejo« le, če je podana osebna privolitev posameznika, pri čemer izraz »obdelujejo« zajema tudi posredovanje le-teh. Glede zbiranja teh podatkov policija privolitve posameznika seveda ne potrebuje, saj četrti odstavek devetega člena ZVOP-1 pravi, da se lahko v javnemu sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, brez privolitve posameznika. Zbiranje podatkov z namenom opravljanja z zakonom določenih nalog pa predpisuje tudi 54. člen Zpol.

Glede posredovanja podatkov je sicer zanimivo tudi mnenje glavnega inšpektorja za varstvo osebnih podatkov, ki ga je v letu 2004 podal Generalni policijski upravi, dotika pa se objavljanja začetnic imena in priimka osumljencev storitve kaznivih dejanj. V tem mnenju je povedal, da lahko policija javnosti posreduje identifikacijske podatke oseb, ki jih obravnava le v primeru, če bi to določal zakon (npr. Zakon o policiji, Zakon o medijih …). Glede na to, da takšnega določila ni, pa je priporočil, da se spremeni način obveščanja javnosti, in sicer tako, da iz njihovih poročil ne bo več mogoče identificirati oseb, na katere se informacije nanašajo.

7.2 (NE)POSREDOVANJE OSEBNIH PODATKOV PRIJAVITELJA KAZNIVEGA DEJANJA

PRITOŽBENI RAZLOGI
Občan je podal pritožbo Informacijskemu pooblaščencu, ker mu Policija in Okrožno državno tožilstvo ne posredujeta podatkov o ovaditelju. Občan je želel, da Pooblaščenec z odločbo naloži Policijski upravi in Okrožnemu državnemu tožilstvu, da se mu omogoči vpogled v kazensko ovadbo.

UGOTOVITVE
Informacijski pooblaščenec je občanu na podlagi predstavljenega dejanskega stanja posredoval neobvezno mnenje:

Policija je dolžna varovati tajnost vira prijave, sporočila oziroma pritožbe, v skladu z drugim odstavkom 56. člena ZPol. Policija bi v primeru, če bi sporočila osebne podatke vira prijave kršila tudi ZVOP-1, saj bi osebne podatke prijavitelja obdelovala v nasprotju z 8. členom ZVOP-1, ki določa splošno opredelitev obdelave osebnih podatkov: osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in

osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.

Pravne podlage za obdelavo osebnih podatkov v javnem sektorju, kamor spada tudi Policija, so navedene v 9. členu ZVOP-1, vendar pa nobena pravna podlaga ne ustreza ravnanju Policije (sporočanje podatka o prijavitelju) v navedenem konkretnem primeru, temveč zakon (ZPol) tako ravnanje celo prepoveduje.

Kar se tiče tožilstva, pravico do vpogleda v kazenski spis ureja več področnih zakonov, na primer Zakon o državnem tožilstvu[27] in Zakon o kazenskem postopku, s spremembami in dopolnitvami.

V skladu s 128. členom ZKP se sme vsakemu, ki ima upravičen interes, dovoliti pregled in prepis posameznih kazenskih spisov. Dokler postopek teče, dovoljuje pregled in prepis spisov organ, pred katerim teče postopek; ko pa je postopek končan, dovoli to predsednik sodišča ali uradna oseba, ki jo on določi. Če so spisi pri državnem tožilcu, dovoljuje pregled in prepis državni tožilec. Pomembno pa je, da se sme pregled in prepis posameznih kazenskih spisov odreči, če to narekujejo posebni razlogi obrambe ali varnosti države ali če je bila javnost izključena z glavne obravnave.

MNENJE
V tem primeru je bilo ravnanje odgovornih na Policiji v skladu z zakoni in veljavnimi predpisi, saj gre tu za načelo, da specialni zakon razveljavi splošnega, se pravi Zpol tukaj razveljavlja ZVOP-1. V drugem odstavku 56. člena ZPol je jasno določeno, da je policist dolžan varovati tajnost vira prijave, sporočila oziroma pritožbe. Te dolžnosti ga lahko razreši le Minister na zahtevo pristojnih organov v utemeljenem primeru, kadar to terjajo interesi izvedbe kazenskega postopka in če s tem ne ogroža življenja ali osebne varnosti posameznika. Tega pa v tem primeru ni.

[27] ZTD-UPB, Uradni list RS, št. 14/2003.

8 ZAKLJUČEK

Varstvo osebnih podatkov se v Sloveniji normativno razvija sicer relativno kratek čas, vendar pa je moje mnenje, da je v tem trenutku že na visokem nivoju. Varstvo podatkov je nasploh, ne smo v policiji, zelo občutljivo področje, tega pa se vse bolj zaveda tudi vsak posameznik. V zadnjem času, ko je vedno več govora o t. i. e-upravi, urejanju upravnih stvari prek interneta, združevanju osebnih podatkov na enem osebnem dokumentu oz. kartici (osebni izkaznici), imajo uporabniki teh storitev vedno bolj v mislih tudi možnosti zlorabe, ki jih do sedaj niso poznali. Tudi zakonodaja v preteklosti temu področju ni namenjala velike pozornosti, z zadnjimi spremembami pa se to vedno bolj uveljavlja.

Tudi v Policiji je situacija podobna. Skozi celotno diplomsko nalogo sem skušal čim bolj natančno predstaviti zakonodajo, ki se je do tega trenutka razvila do te mere, da lahko učinkovito ščiti posameznika pred posegi policije v pravice, povezane z njegovimi osebnimi podatki. V Policiji se obdeluje ogromno osebnih podatkov, tako preko računalniških kot drugih evidenc. Tega so se zavedli tudi odgovorni posamezniki v sami organizaciji in poskušali sestaviti podzakonske akte, ki stvari čim bolj eksaktno urejajo in določajo.
Pravilnik o varovanju podatkov policije in drugi sorodni akti so bili napisani z mislijo, da se posameznika zaščiti pred zlorabami in se čim bolj natančno določi, kaj vse je dovoljeno in kaj ne. Zaostrujejo se tudi pogoji za dostop do baz osebnih podatkov, uporaba gesel in nadzor do dostopa. Uporabnik je že ob vstopu v evidence opozorjen, da se vsi dostopi do podatkov beležijo, ob tem pa so taksativno našteti zakoni in drugi predpisi oz. njihovi deli, ki dostop urejajo. Sistem evidenc in baz podatkov pa je ob tem zasnovan tako, da se ob daljši neuporabi sam izključi oz. zaklene, s tem pa prepreči zlorabo.

V prejšnjem poglavju sta opisana dva različna primera.
V prvem primeru so odgovorni na Policiji storili napako in posredovali osebne podatke, ki jih ne bi smeli. Po pritožbi občana na enega izmed pristojnih organov, Varuha človekovih pravic, je stekel postopek, opredeljen v zakonu, odgovornim pa je bila predočena kršitev in izrečeno opozorilo.
V drugem primeru pa odgovorni na Policiji niso posredovali zahtevanih podatkov, češ da to ne bi bilo zakonito. Tudi v tem primeru se je občan pritožil na pristojni organ, tokrat je bil to Informacijski pooblaščenec, ta pa je v svojem mnenju podprl ravnanje Policije.

Iz teh primerov lahko izvlečemo več stvari. Jasno je, da se v Policiji, tako kot v drugih organizacijah, zgodijo napake oz. kršitve. Te so lahko namerne ali nenamerne, posledica neznanja ali malomarnosti, kar pa niti ni tako pomembno. Pomembno ob tem je, da imamo zakonodajo, ki posameznika v takih primerih ščiti. Pomembno je, da obstajajo institucije, ki v primerih očitanih zlorab in nepravilnosti stvari preverijo in ukrepajo. V Policiji so stvari sicer dobro urejene, upam si celo trditi, da je Policija

glede varstva osebnih podatkov eden bolj urejenih organov v RS, vendar po kot organ ni samozadostna. Obstoj drugih organizacij, ki preverjajo njeno delovanje, je tako nujen. Le sistem, ki deluje kot celota, lahko deluje dobro in učinkovito preprečuje morebitne kršitve in zlorabe.

LITERATURA

1. BOGATAJ, Jože. Varstvo osebnih podatkov. Ministrstvo za pravosodje RS, Ljubljana, 2008.

2. CERAR, Miro. Temelji ustavne ureditve, človekove pravice in temeljne svoboščine, gospodarska in socialna razmerja (učno gradivo za udeležence seminarja). Ministrstvo za notranje zadeve, Direktorat za javno upravo, Upravna akademija, Ljubljana, 2004.

3. ČEBULJ, Janez. Varstvo osebnih podatkov z zakonskimi pooblastili. Inštitut za javno upravo pri Pravni fakulteti v Ljubljani, Ljubljana, 1990.

4. ČEBULJ, Janez; ŽUREJ, Jurij. Varstvo osebnih podatkov in informacije javnega značaja. Nebra, Ljubljana, 2005.

5. DEISINGER, Mitja. Kazenski zakonik s komentarjem, Ljubljana, 2002.

6. KAUČIČ, Igor. Ustavna ureditev Slovenije. Ljubljana, GV Založba, 2003.

7. KOCJANČIČ, Rudi. Človekove pravice in temeljne svoboščine. Ustavno pravo Slovenije. Visoka upravna šola, Ljubljana, 1998.

8. PIRC MUSAR, Nataša. Zakon o varstvu osebnih podatkov (ZVOP-1), s komentarjem, Ljubljana, 2006.

9. PRPELUH, Urška. Pravica dostopa do informacij javnega značaja. Pravna fakulteta Univerze v Ljubljani, Ljubljana 2005.

10. TRPIN, Gorazd. Varuh človekovih pravic in temeljnih svoboščin. Nova ustavna ureditev Slovenije, zbornik razprav. Uradni list RS, Ljubljana, 1992.

11. VIRANT, Gregor. Nadzor nad delovanjem uprave: Pravna ureditev javne uprave. Fakulteta za upravo, Univerza v Ljubljani, Ljubljana, 2004.

VIRI

1. Ustava RS. UL RS, št. 33/1991-I, 42/1997, 66/2000, 24/2003 in 69/2004.

2. Evropska konvencija o človekovih pravicah (EKČP). UL RS – Mednarodne pogodbe, št. 7–41/1994, UL RS št. 33/1994.

3. Direktiva 95/46/ES Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku podatkov, 14. 10. 1995. OJ 1995/L 281, UL Evropskih skupnosti, št. L 281, 23. 11. 1995.

4. Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov 1981 (Konvencija, št. 108). UL RS, št. 11/1994 – Mednarodne pogodbe, št. 3/1994.

5. Kazenski zakonik RS. UL RS, št. 63/1994.

6. Zakon o dostopu do informacij javnega značaja (ZDIJZ). UL RS, št. 24/2003, 61/2005, 109/2005, 28/2006 (UPB2).

7. Zakon o inšpekcijskem nadzoru (ZIN). UL RS, št. 56/2002.

8. Zakon o tajnih podatkih (ZTP). UL RS, št. 87/2001, 135/2003 (UPB1), 28/2006.

9. Zakon o varuhu človekovih pravic (ZVarČP). UL RS, št. 71/1993, 15/1994.

10. Zakon o varstvu osebnih podatkov (ZVOP-1). UL RS, št. 86/2004.

11. Zakon o prekrških (ZP-1), UL RS, št. 55/2005, 70/2006.

12. Zakon o policiji (Zpol). UL RS, št. 49/1998, 93/2001, 56/200298/2005.

13. Pravilnik o varovanju podatkov policije (UL RS, št. 79/1999).

SPLETNE STRANI

Spletna stran Informacijskega pooblaščenca RS:
URL = http://www.ip-rs.si/; URL = http://www.ip-rs.si/pristojnosti/; URL = http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/;

Spletna stran Varuha človekovih pravic:
URL= http://www.varuh-rs.si/; URL = http://www.varuh-rs.si/index.php?id=44;

Spletna stran Ministrstva za notranje zadeve:
URL = http://www.mnz.gov.si/; URL = http://www.mnz.gov.si/si/slovenija_in_schengen/;

Spletna stran Policije:
URL = http://www.policija.si/portal/; URL = http://www.policija.si/portal/ijz/evidence/evidence.php, intranet policije URL = http://intranet.policija.si;

Spletna stran Uradnega lista RS:
URL = http://www.uradni-list.si/

Spletna stran javne uprave, e-uprave:
URL = http://e-uprava.gov.si/e-uprava/portal.euprava in URL = http://e-uprava.gov.si/e-uprava/portalStran.euprava?pageid=42

PRILOGA 1

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
P O L I C I J A

ORGANIZACIJSKA ENOTA

Številka:
Datum:

Na podlagi 6. člena Pravilnika o varovanju podatkov policije (številka: 007-229/2008, z dne 31.5.2008) izdajam

O D L O Č B O

s katero določam _____ *ime in priimek* _____, *delovno mesto*_____, za vodjo lokalnega informacijskega sistema na _____*organizacijska enota*____.
Vodja lokalnega informacijskega sistema je delavec policije, ki je odgovoren za obravnavanje podatkov v okviru lokalnega informacijskega sistema.
S to odločbo preklicujem odločbo ___*številka*_____ z dne _____, s katero je bil za vodjo LIS
na ____*organizacijska enota*____ določen _____*ime in priimek*_____.

Odločba velja takoj.

Vodja enote
Naziv

Poslano:
1. Ime in priimek
2. MNZ RS - POLICIJA
3. Arhiv

PRILOGA 2

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
P O L I C I J A
Štefanova ulica 2, 1501 LJUBLJANA
Telefon: 01 428 40 00; telefaks: 01 428 47 33
E-pošta: gp.mnz@gov.si; http://www.policija.si

Številka:
Datum:

Na podlagi 3. člena Pravilnika o varovanju podatkov Policije (številka: 007-229/2008, z dne 31.5.2008) ter 15. člena Pravilnika o hrambi podatkov o elektronskih komunikacijah policije in o
dostopu do policijskih zbirk podatkov (Uradni list RS, št. 103/06, 59/07) podpisani(-a)

_____
(ime in priimek, EMŠO)
_____
(ulica, kraj bivanja, poštna številka, pošta)
_____-
(organizacijska enota)

I Z J A V L J A M

da sem seznanjen(-a) s predpisi, ki v Policiji urejajo varstvo in varovanje podatkov.

Ob podpisu izjave sem bil(-a) posebej seznanjen(-a):

☐ da lahko delavec policije varovane podatke uporablja le za opravljanje z zakonom določenih nalog in skladno z navodili, ki urejajo način obravnavanja posameznih podatkov *(Pravilnik o varovanju podatkov policije, št.:007-229/2008, z dne 31.5.2008 in Zakon o Policiji, Uradni list RS, št. 107/06 uradno prečiščeno besedilo; **ZPol**)*,

☐ da se obravnavanje podatkov in uporaba opreme informacijskega in telekomunikacijskega sistema policije (ITSP) evidentira v dnevnikih dela ITSP, katerih zapisi so namenjeni preverjanju upravičenosti obravnavanja podatkov in uporabe opreme ITSP ter preiskovanju sumov kršitev varstva in varovanja podatkov policije,

☐ da se smejo osebni podatki obdelovati samo za namene, določene z zakonom, in ne smejo biti uporabljeni na način, ki ni združljiv s temi nameni. Pri obdelavi je dolžan vsak uporabnik, skladno s svojimi delovnimi nalogami, skrbeti za vestno, strokovno in ažurno obdelavo, obdelava pa je dovoljena samo z uporabo uporabnikovega osebnega gesla. *(Pravilnik o načinu vodenja policijskih evidenc, Uradni list RS, št. 121/04, 51/07)*,

☐ z določili IV. poglavja ZPol (zbiranje, varstvo in zavarovanje podatkov),
☐ na določila Zakona o varstvu osebnih podatkov *(Uradni list RS, št. 94/07 - uradno prečiščeno*

*besedilo; **ZVOP-1**),*

- na določila Pravilnika o varovanja podatkov policije,
- na določila Pravilnika o načinu vodenja policijskih evidenc,
- na določila Kazenskega zakonika Republike Slovenije (Uradni list RS, št. 63/94, 70/94, 23/99, 40/04, 95/04), ki določajo kazniva dejanja izdaje državne, uradne, vojaške in poslovne tajnosti ter kaznivo dejanje zlorabe osebnih podatkov,
- da dolžnost varovanja podatkov ne preneha s prenehanjem delovnega razmerja v policiji *(Pravilnik o načinu vodenja policijskih evidenc, Uradni list RS, št. 121/04, 51/07)*.

V _____, dne _____

PODPIS:

PRILOGA 3

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
P O L I C I J A
Štefanova ulica 2, 1501 LJUBLJANA
Telefon: 01 428 40 00; telefaks: 01 428 47 33
E-pošta: gp.mnz@gov.si; http://www.policija.si

I Z J A V A

Spodaj podpisani,_____, rojen_____, v _____, stanujoč_____, _____, sem seznanjen z zahtevo Ministrstva za notranje zadeve - Policije, da podatke, vezane _____, varujem, skladno z določili Zakona o varstvu osebnih podatkov (ZVOP-1, Uradni list RS, št. 86/04, 113/05, 67/07), Pravilnika o varovanju podatkov policije (številka: 007-229/2008, z dne
31.5.2008) in drugimi predpisi s področja varstva podatkov, kot URADNO TAJNOST in da razkritje teh podatkov nepooblaščenim osebam pomeni storitev kaznivega dejanja 'izdaja uradne tajnosti'.

Podpis: _____

9 IZJAVA O AVTORSTVU IN NAVEDBA LEKTORJA

Študent Simon LIKAR, številka indeksa 04031871, izjavljam, da sem avtor diplomskega dela z naslovom Varstvo osebnih podatkov v policiji in dovoljujem objavo dela na internetu.

Diplomsko delo je lektorirala Zdenka LIKAR, učiteljica slovenskega jezika.

Kranj, 08.01.2009 Podpis: