Smernice glede uvedbe biometrijskih ukrepov

Priročnik, ki vam bo pojasnil pravila, kdaj in pod katerimi pogoji lahko upravljavci osebnih podatkov uvedejo biometrijske ukrepe in na kaj morajo ob tem paziti.

INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo odgovore na najpogosteje zastavljena vprašanja z vidika zahtev Zakona o varstvu osebnih podatkov glede uvedbe biometrijskih ukrepov, kot so: pod kakšnimi pogoji so biometrijski pogoji dopustni, ali gre pri tem za obdelavo osebnih podatkov, kakšen je postopek pridobitve dovoljenja Pooblaščenca in druga.
Ciljne javnosti:	Subjekti javnega in zasebnega sektorja, ki razmišljajo o uvedbi biometrijskih ukrepov.
Status:	javno
Verzija:	1.0
Datum verzije:	29. 2. 2008
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, biometrija, javni sektor, zasebni sektor, biometrijska značilnost, prstni odtisi, odločba, evidentiranje delovnega časa in prisotnosti na delovnem mestu, nadzor dostopa.

VSEBINA

> > >

O smernicah Informacijskega pooblaščenca (IP)

Namen smernic IP je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1-UPB1).

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1-UPB1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- *Mnenja IP*:
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/

- *Brošure IP*:
  http://www.ip-rs.si/publikacije/prirocniki/

Smernice IP so objavljene na spletni strani:

http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Uvod

Biometrija v sodobnem svetu pridobiva na pomenu, družbe pa so se glede dolgoročnega odnosa do biometrije znašle pred pomembnimi odločitvami. Uporaba biometrije vsekakor narašča in jo lahko zasledimo v številnih dejavnostih, uporablja pa se za različne namene: obramba, nacionalna varnostna in obveščevalna dejavnost, upravljanje zaporov, ukrepi na državnih mejah, imigracij, potni listi, bančne in finančne institucije, informacijski sistemi… Biometrija ima nedvomno z vidika posameznika določene praktične prednosti. Kot vsaka druga tehnologija se tudi biometrija lahko uporabi na način, ki je prijazen do zasebnosti posameznika, lahko pa gre za občutne posege v zasebnost posameznika in učinek »velikega brata«. Praktične prednosti biometrije so praviloma vidne na prvi pogled, medtem ko nekateri vidiki, ki dokazujejo, da tudi biometrija ni vsemogočna in popolna, niso vidni na prvi pogled. Biometrijski ukrepi so po naravi stvari takšni, da pomenijo velik poseg v zasebnost in dostojanstvo posameznika, zato je treba vse pogoje za njihovo uporabo razlagati v luči njune zaščite in izhajati ZVOP-1 –UPB1, s katerim se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov.

Namen pričujočih smernic je pojasniti nekatere osnovne značilnosti biometrijskih ukrepov, pojasniti nekatere dileme glede obdelave osebnih podatkov v sklopu biometrijskih ukrepov, predstaviti zakonsko ureditev teh ukrepov ter podati odgovore na najpogosteje zastavljena vprašanja s katerimi se srečujejo subjekti javnega in zasebnega sektorja, ki razmišljajo o uvedbi biometrije.

Splošno o biometriji

Kaj je biometrija?

Sama beseda biometrija izhaja iz starogrške besede »bios« (življenje) in »metron« (meritev). Poenostavljeno bi lahko rekli, da je biometrija ali biometrika, kot včasih tudi zasledimo, veda o načinih prepoznave ljudi na podlagi njihovih telesnih, fizioloških ter vedenjskih značilnosti, ki jih imajo vsi posamezniki, ki so hkrati edinstvene in stalne za vsakega posameznika posebej in je možno z njimi določiti posameznika, zlasti z uporabo prstnega odtisa, posnetka papilarnih linij s prsta, šarenice, očesne mrežnice, obraza, ušesa, DNK ter značilne drže.

Telesna podatka sta sicer na primer tudi teža in višina osebe, vendar ta dva nista biometrični značilnosti, ker ne omogočata unikatnega ločevanja oseb oziroma nista primerna za določljivost posameznika. Določen telesni, fiziološki ali vedenjski podatek je primeren za določevanje posameznika, če za posameznika deluje kot neke vrste »individualno geslo« in s tem omogoča zanesljivost in točnost biometrijskih ukrepov.

Biometrija je danes samo eden izmed načinov ugotavljanja oz. preverjanje identitete. Preostali načini so znani že dalj časa. Gre za načine, ki temeljijo na »tistemu, kar oseba ima« (npr. magnetna kartica), ali pa temeljijo na »tistemu, kar oseba ve« (osebno geslo, PIN-koda). Biometrija sodi v tretjo skupino, ki temelji na »tistemu, kar oseba je«. Gre torej za neko samo njej lastno telesno oziroma vedenjsko značilnost. Takšen način preverjanja ima lahko pred ostalima določene prednosti z vidika praktičnosti in varnosti. Magnetne kartice se izgubijo, ukradejo, posodijo, osebna gesla se pozabijo, razkrijejo ipd., biometrične značilnosti pa ostanejo (vsaj načeloma) večne, ne morejo se izgubiti ali pozabiti, težko jih je reproducirati oziroma prenesti na drugo osebo.

Katere človeške značilnosti se v biometriji najpogosteje uporabljajo?

Naštejmo le najbolj znane. Lahko jih ločimo na telesne in vedenjske značilnosti:

Vedenjske značilnosti:

- lastnoročno podpisovanje,
- govor (glas),
- gibanje,
- tipkanje.

Telesne značilnosti:

- prstni odtis,
- dlan,
- podoba obraza,
- šarenica,
- očesna mrežnica
- uho,
- preplet ven na roki,
- vonj,
- DNK.

Niso vse biometrične značilnosti enako neponovljive oziroma unikatne. Kot najbolj unikatne se štejeta očesna mrežnica in DNK. Vendar unikatnost ni absolutna. Tako je npr. zanimiv primer uporabe biometrije iz Velike Britanije. V primeru Raymond Easton proti Veliki Britaniji se je izkazalo, da imata lahko dve osebi enak celo del zapisa DNK (v konkretnem primeru na šestih mestih), za kar je sicer teoretično izračunana verjetnost kar 1:37.000.000. Zato je na mestu opozorilo, da biometrija tudi s tega vidika ni vsemogočen in nezmotljiv način identifikacije in ji zato ne gre slepo zaupati.

Kako delujejo biometrijske naprave?

Za zajem značilnosti vzorca prstnega odtisa obstaja več algoritemskih metod.

Vzemimo primer prstnih odtisov kot najpogosteje uporabljene biometrijske metode. Najbolj razširjene metode temeljijo na prepoznavanju vzorca ali izvlečku minucij. V primeru algoritmov, ki temeljijo na minucijah, je prstni odtis sestavljen iz grobih značilnosti, kot so loki, zanke in zasuki, ter drobnih značilnosti (minucije) kot so predvsem bifurkacije (razdelitve), delte (združevanja v obliki črke Y) in zaključki grebenov. Prstni odtis ima med 30 in 40 minucij. Značilnost vsake od njih je položaj (koordinate), tip (bifurkacija, delta ali zaključek) in usmerjenost (orientacija). Skupek značilnosti minucij lahko da predlogo za prstni odtis. Če so značilnosti natančno zajete, je možnost, da bi imela dva prstna odtisa enake značilnosti, izjemno nizka.

Animirani prikaz principov delovanja biometrijskih naprav si lahko ogledate na tej spletni strani:

http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/default.stm.

ZVOP-1 pod pojmom »biometrijskih ukrepov« zajema dva različna načina (postopka) prepoznave posameznika:

*1. postopek, s katerim se ugotavljajo lastnosti posameznika, tako da se lahko izvrši njegova **identifikacija**;*

*2. postopek, s katerim se primerjajo lastnosti posameznika, tako da se lahko preveri njegova identiteta oziroma istovetnost (**avtentikacija**).*

Iz tega je razvidno, da zakon sicer loči med izvrševanjem identifikacije (prepoznava) in preverjanjem identitete posameznika (istovetnost ali avtentikacija), vendar za oba postopka uporablja enoten termin – biometrijski ukrep.

Identifikacija išče odgovor na vprašanje »*Kdo sem?*«, avtentikacija pa na vprašanje »*Ali sem tisti, za katerega se predstavljam?*«.

Razliko lahko pojasnimo tudi drugače. Postopek preverjanja identitete (avtentikacija) ugotavlja, ali je oseba res ta, za katero se izdaja. Oseba mora najprej sistemu sporočiti, za koga se izdaja. To stori npr. z brezkontaktno kartico ali z vnosom osebnega gesla in hkrati ponudi tudi svojo biometrično značilnost (npr. prstni odtis). Sistem nato izvede primerjavo med to ponujeno biometrično značilnostjo in že prej shranjenim biometričnim podatkom, ki pripada tistemu, za katerega se sedaj ta oseba izdaja. Sistem izvede torej primerjavo 1:1 in lahko odgovori le z DA ali NE. Torej ali je oseba res ta, za katero se izdaja, ali pa to ni. Na ta način se torej preveri identiteta.

Postopek identifikacije poteka drugače. V tem postopku se ne preverja, ali je oseba res ta, za katero se izdaja, temveč sistem sam ugotavlja identiteto osebe. Oseba zgolj ponudi biometrično značilnost in sistem poišče v bazi že prej shranjenih biometričnih podatkov ustrezen par. Če ga najde, se identifikacija izvrši, drugače ne. Izvede torej 1:N operacijo, pri čemer N predstavlja vse že prej shranjene biometrične podatke.

Sistem identifikacije vedno vključuje centralno zbirko biometričnih podatkov, sistem avtentikacije pa ne nujno. Tipičen primer sistema identifikacije je iskanje storilcev kaznivih dejanj na podlagi npr. prstnih odtisov. Podatke o prstnem odtisu, najdenem na kraju zločina, vnesejo v sistem, ki jih nato primerja z vsemi že prej shranjenimi podatki. Če najde par, je oseba identificirana.

Zakaj uporaba biometrije narašča?

Vse več je zahtev po avtomatiziranem, natančnem in hkrati hitrem ugotavljanju oz. potrjevanju identitete posameznika. Vse več je tudi aplikacij avtomatiziranega odločanja o pravicah in dolžnostih posameznika, tudi zaradi prednosti biometričnih značilnosti, ki so:

- unikatne,
- neprenosljive na drugo osebo,
- ni jih mogoče pozabiti ali izgubiti,
- težko jih je kopirati ali ponarediti,
- lahko se uporabijo z vednostjo ali brez vednosti posameznika,
- posamezniku jih je težko spremeniti ali skriti.

Kako je biometrija urejena pri nas?

Zakon, ki ureja varstvo osebnih podatkov (ZVOP-1), ureja v posebnem poglavju (78. do 81. člen) biometrijske ukrepe kot posebno vrsto obdelave osebnih podatkov:

Splošna določba - 78. člen
Z obdelavo biometričnih značilnosti se ugotavljajo ali primerjajo lastnosti posameznika, tako da se lahko izvrši njegova identifikacija oziroma preveri njegova identiteta (v nadaljnjem besedilu: biometrijski ukrepi) pod pogoji, ki jih določa ta zakon.

Biometrijski ukrepi v javnem sektorju - 79. člen
(1) Biometrijske ukrepe v javnem sektorju se lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

(2) Ne glede na prejšnji odstavek se biometrijske ukrepe lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja.

Biometrijski ukrepi v zasebnem sektorju - 80. člen
(1) Zasebni sektor lahko izvaja biometrijske ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Biometrijske ukrepe lahko izvaja le nad svojimi zaposlenimi, če so bili predhodno o tem pisno obveščeni.

(2) Če izvajanje določenih biometrijskih ukrepov v zasebnem sektorju ni urejeno z zakonom, je upravljavec osebnih podatkov, ki namerava izvajati biometrijske ukrepe, dolžan pred uvedbo ukrepov posredovati državnemu nadzornemu organu opis nameravanih ukrepov in razloge za njihovo uvedbo.

(3) Državni nadzorni organ je po prejemu posredovanih informacij iz prejšnjega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometrijskih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se lahko podaljša za največ en mesec, če bi uvajanje teh ukrepov prizadelo več kot 20 zaposlenih v osebi zasebnega sektorja, ali če reprezentativni sindikat pri delodajalcu zahteva sodelovanje v upravnem postopku.

(4) Upravljavec osebnih podatkov sme izvajati biometrijske ukrepe po prejemu odločbe iz prejšnjega odstavka, s katero je izvajanje biometrijskih ukrepov dovoljeno.

(5) Zoper odločbo državnega nadzornega organa iz tretjega odstavka tega člena ni pritožbe, dovoljen pa je upravni spor.

Biometrijski ukrepi v zvezi z zaposlenimi v javnem sektorju - 81. člen
Ne glede na določbe 79. člena tega zakona se v javnem sektorju lahko uvedejo biometrijski ukrepi v zvezi z vstopom v stavbo ali dele stavbe in evidentiranjem prisotnosti zaposlenih na delu, ki se izvedejo ob smiselni uporabi drugega, tretjega in četrtega odstavka 80. člena tega zakona.

Zakon torej dovoljuje uporabo biometrije le v naslednjih primerih:

- za **JAVNI SEKTOR**: kadar tako določa zakon (npr. Zakon o potnih listinah državljanov Republike Slovenije), izjemoma na podlagi posebnih zakonskih določil tudi za vstop v stavbo ali dele stavb in evidentiranje zaposlenih na delu.

- za **ZASEBNI SEKTOR**: le, če so nujno potrebni za:
  - opravljanje dejavnosti,
  - varnost ljudi ali premoženja,
  - varovanje tajnih podatkov ali
  - varovanje poslovne skrivnosti.

Zasebni sektor lahko biometrijske ukrepe izvaja le nad svojimi zaposlenimi, če so bili ti o tem predhodno obveščeni, vendar je tu potrebno opozoriti, da obveščenost zaposlenih ni zadostni, temveč zgolj potrebni pogoj za uvedbo biometrijskih ukrepov.

Če izvajanje biometrijskih ukrepov v zasebnem sektorju ni določeno z zakonom, mora tisti, ki želi uvesti biometrijske ukrepe, pridobiti odločbo Informacijskega pooblaščenca.

Zakaj je področje biometrije urejeno v Zakonu o varstvu osebnih podatkov (ZVOP-1)?

Prstni odtis, podobno kot šarenica, očesna mrežnica, obraz ipd, so biometrični podatki in kot taki tudi nedvomno osebni podatki, saj gre za takšne značilnosti, ki so edinstvene in stalne za vsakega posameznika posebej in na podlagi katerih je oseba določena oziroma vsaj določljiva. Zato se vsakršno zbiranje, shranjevanje, pošiljanje, uničevanje ipd. teh podatkov šteje za obdelavo osebnih podatkov in posledično zanje veljajo določbe zakona, ki ureja varstvo osebnih podatkov, torej ZVOP-1.

Kaj pa vzorci (template), ki se uporabljajo v sodobnih biometrijskih sistemih. Ali gre tudi tu za osebne podatke?

Osebni podatek je katerikoli podatek, ki se nanaša na točno določeno ali vsaj določljivo osebo, ne glede na obliko, v kateri je izražen. Oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno ipd. identiteto, pri čemer je način identifikacije razumno dosegljiv ne samo upravljavcu, temveč tudi kateri koli drugi osebi. Biometrični podatek je po naravi stvari vedno podatek, ki se nanaša na točno določeno ali vsaj določljivo osebo. Podatki o npr. prstnem odtisu vedno pripadajo točno določeni osebi. Ali to velja tudi za biometrične podatke, ki so shranjeni v reducirani, digitalizirani obliki (template)?

Svet Evrope je v svojem poročilu zapisal, da dilema, ali so biometrični podatki vedno osebni podatki ali le, če so izpolnjeni določeni pogoji, ni relevantna. Namreč, če so biometrični podatki zbrani z namenom kasnejše avtomatske obdelave, vedno obstaja možnost, da bodo ti podatki povezani z določeno ali določljivo osebo, kar ustreza definiciji osebnih podatkov.

Kar velja za biometrične značilnosti kot take, velja tudi za digitalen zapis teh značilnosti, ki so sestavljeni na podlagi unikatnih značilnosti, ne glede na to, kolikokrat in kako je ta zapis kasneje spremenjen. Ne glede na obliko, način zapisa ali drugo spremembo, ostane vedno tista edinstvena vez z osebo, četudi se morebiti količina podrobnosti v postopku transformacije zmanjšuje.

Na podlagi tega lahko rečemo, da so biometrični podatki, četudi shranjeni v reducirani, digitalizirani obliki, vedno osebni podatki, saj se nanašajo na določeno ali vsaj določljivo osebo.

Ali se biometrične značilnosti vedno štejejo za občutljive osebne podatke?

Ne. Biometrične značilnosti se sicer lahko tudi štejejo za občutljive osebne podatke, vendar le, če je z njihovo uporabo mogoče določiti posameznika v zvezi s tistimi lastnostmi, ki jih zakon našteva kot občutljive osebne podatke (predvsem podatki o rasnem, narodnem ali narodnostnem poreklu ali zdravstvenem stanju).

Biometrija in zdravstveno stanje?

Kot kažejo raziskave, se pri nekaterih ljudeh pojavlja strah, da bi lahko nekateri biometrični ukrepi bili zdravju škodljivi. V tej zvezi se omenja npr. uporaba infrardeče svetlobe pri snemanju očesne mrežnice ali infekcijski problemi pri skeniranju prstnih odtisov. Takšnih primerov v praksi ni veliko.

Bolj pomembni so podatki o zdravstvenem stanju, ki jih »skrivajo« biometrični podatki. Ti namreč lahko o osebi razkrijejo bistveno več, kot bi si ta oseba želela oziroma je pristala takrat, ko se je zbiranje izvedlo. Tako je mogoče na podlagi DNK vzorca ugotoviti ne le identitete posameznika, temveč tudi njegovo zdravstveno stanje, morebitne genske okvare ipd. Znanstveniki s področja iridiologije, vede, ki preučuje značilnosti očesne šarenice, pa trdijo, da se tudi iz šarenice da razbrati zdravstveno stanje. Podobno velja glede identifikacije glasu. Glas poleg identifikacije lahko sporoča tudi čustveno stanje. To pa je s stališča varstva osebnih podatkov problematično. Lahko si zamislimo primer, ko podjetje uvede kontrolo vstopa v prostor s pomočjo značilnosti glasu zaposlenih. Biometrični podatek (glas) se v tem primeru uporabi za preverjanje oziroma ugotavljanje identitete za namene vstopa v prostor. Predpostavimo nadalje, da podjetje kasneje prične uporabljati tako zbrane biometrične podatke tudi za preverjanje čustvenega stanja zaposlenih ali za stalno preverjanje njihove fizične lokacije. Podjetje bi torej uporabilo biometrične značilnosti za namene, ki so v neskladju z nameni, zaradi katerih so bilidovoljeni. V tem primeru bi podjetje kršilo temeljno načelo, zapisano v 16. členu ZVOP-1, ki določa, da se osebni podatki ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju z nameni, zaradi katerih so se zbrali.

Zdravstveno stanje je lahko tudi ovira za uporabo biometrije. To se zgodi pri osebah brez nekaterih biometričnih značilnosti (aniridia; “suh” prstni odtis oz. odtis brez značilnosti) ali tudi pri npr. poškodbah obraza, ko sistem za prepoznavo obraza (t. i. face recognition) več ne prepozna osebe.

Pogosto zastavljena vprašanja

V tem poglavju najdete odgovor na najpogosteje zastavljena vprašanja, s katerimi se srečujejo podjetja in organizacije v zasebnem sektorju, ki razmišljajo o uvedbi biometrijskih ukrepov.

Kaj naj delodajalec v zasebnem sektorju upošteva, če želi uvesti biometrijske ukrepe?

Delodajalec mora ugotoviti, zakaj pravzaprav želi uvesti biometrijske ukrepe, torej kakšni so nameni, ki jih želi s tem doseči. Ti nameni morajo biti resni, utemeljeni in podprti z dokazi, predvsem pa mora presoditi, ali so nujno potrebni za opravljanje dejavnosti, varovanje premoženja, ljudi ali za varovanje tajnih podatkov ali poslovnih skrivnosti (80. člen ZVOP-1). Pred uvedbo biometrijskih ukrepov mora skrbno pretehtati, ali bi drug način preverjanja identitete, ki ne vključuje biometrije, zadovoljivo dosegel namen, ki ga zasleduje.
Preden zaprosi Informacijskega pooblaščenca za izdajo odločbo za odobritev izvajanja biometrijskih ukrepov in še pred morebitnim nakupom biometrijske naprave oz. čitalnika, , se mora odločiti, kakšen sistem bo uvedel. Ali bodo biometrični podatki shranjeni centralno, razpršeno (npr. na kartici, ki jo ima vsak zaposleni) ali bo sistem temeljil na identifikaciji ali avtentikaciji itn. Bolj, ko sistem posega v zasebnost posameznika (vključuje tudi vprašanje možnosti zlorab), bolj resen in utemeljen razlog za uvedbo biometrijskih ukrepov mora upravljavec imeti. To vključuje tudi tehnične vidike. Irski nadzorni organ za varstvo osebnih podatkov je na svoji spletni strani (www.dataprotection.ie) objavil več zelo dobrodošlih vprašanj, na katera bi moral delodajalec odgovoriti pred uvedbo biometrijskih ukrepov:

1. *Ali že imamo vzpostavljen sistem za evidentiranje prisotnosti zaposlenih na delu in/ali sistem za kontrolo vstopov v prostore?*
2. *Zakaj ga želimo zamenjati?*
3. *Kakšne so poglavitne slabosti tega sistema?*
4. *Ali so slabosti posledica nepopolnega izvajanja ali so neločljivo povezane z naravo samega sistema?*
5. *Ali smo preverili več različnih tipov sistemov, ki bi prišli v poštev za naše potrebe?*
6. *Ali bi sistemi, ki ne vključujejo biometrijskih ukrepov, zadovoljivo izpolnili naše potrebe?*
7. *Ali potrebujemo sistem, ki vključuje biometrijske ukrepe?*
8. *Če ga potrebujemo, kakšne vrste sistema potrebujemo?*
9. *Ali potrebujemo sistem, ki temelji na ugotavljanju identitete, ali sistem, ki temelji na preverjanju identitete (avtentikacija)?*

10. Ali potrebujemo centralno zbirko biometričnih podatkov?
11. Ali bi lahko sistem temeljil tudi na decentraliziranem shranjevanju biometričnih podatkov?
12. Kakšne namene pravzaprav želimo doseči z biometrijskimi ukrepi?
13. Ali ga potrebujemo za evidentiranje prisotnosti zaposlenih na delu ali/in za kontrolo vstopa v prostore (fizične in informacijske)?
14. Kako natančno želimo zajeti biometrične podatke?
15. Kakšni so postopki za zagotavljanje točnosti in ažurnosti biometričnih podatkov?
16. Ali je biometrične podatke, ki jih bomo shranjevali, potrebno ažurirati?
17. Kakšni so postopki in načini za zavarovanje biometričnih podatkov?
18. Kdo bo imel dostop do biometričnih podatkov?
19. Zakaj, kdaj in pod katerimi pogoji bo do teh podatkov mogoč dostop?
20. Kaj se bo štelo za zlorabo sistema s strani zaposlenih?
21. Kakšne bodo postopki za ugotavljanje ali je šlo za zlorabo ali le za napako?
22. Ali bo sistem poleg biometrijskih ukrepov temeljil še na kakšnem dodatnem načinu ugotavljanja oz. preverjanja identitete (osebna gesla, brezkontaktne kartice ipd.)
23. Če bo, ali bi ti dodatni načini ugotavljanja oz. preverjanja identitete zadovoljivo izpolnili namene, ki jih zasledujemo tudi brez biometrijskih ukrepov?
24. Kako bomo obvestili vse zaposlene o uvedbi biometrijskih ukrepov?
25. Katere informacije bomo posredovali zaposlenim?

Na koncu pa še nasvet, ki sicer ni strogo vezan na varstvo osebnih podatkov, je pa gotovo dobrodošel za ohranitev vsaj delčka humanosti tudi na delovnem mestu. Delodajalec naj upošteva tudi, da morajo biti pravice zaposlenega, ki je v prvi vrsti človek in ne zgolj delavec, spoštovane tudi na delovnem mestu in da številne raziskave kažejo, da pretirano uvajanje nadzora nad zaposlenimi ne škoduje samo zaposlenim, temveč škoduje tudi uspehu podjetja. Tako se je npr. v raziskavah, opravljenih v Kanadi (predstavljene na konferenci Infonex 2001 - Reasonableness in the Context of Workplace Privacy) pokazalo, da obstaja tesna povezanost med nadzorom zaposlenih in stresom in da je to v končni posledici dražje za podjetje zaradi odsotnosti zaradi bolezni in tudi zaradi predčasnih odhodov delavcev iz podjetja. Izkušnje namreč potrjujejo, da je v delovnih okoljih koristneje sredstva nameniti razvijanju primernih medosebnih odnosov, vzpostavljanju spodbudnega delovnega okolja, zaupanju ter krepitvi pripadnosti kolektivu, kakor pa vseobsežnemu nadzoru zaposlenih s tehničnimi sredstvi. Ali v drugih besedah: Za reševanje družbenih težav ne bi smeli uporabljati tehničnih sredstev“ (v originalu: We should not be trying to use technical solutions to solve a social problem). Nadzor v kolektiv vnaša nemir in nezadovoljstvo ter ruši zaupanje in pozitivno vzdušje. Primeri iz ameriške in evropske sodne prakse dokazujejo, da prihaja tudi do zlorab nadzornih sistemov s strani nadrejenih (Aljaž Marn, Dnevnik nove ekonomije).

Ali lahko v podjetju uvedemo biometrijo za evidentiranje delovnega časa zaposlenih?

Po določbi 80. člena ZVOP-1 se biometrijski ukrepi lahko izvajajo le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. S takšno določbo je zakonodajalec sledil načelu sorazmernosti (3. člen ZVOP-1) in načelo konkretiziral glede obdelave posebne vrste osebnih podatkov, t.j. biometričnih podatkov ter s tem omejil možnosti prekomernih in neupravičenih posegov v zasebnost in dostojanstvo posameznika pri izvajanju biometrijskih ukrepov. Obstajati mora torej resnično upravičen razlog, ki terja, da je biometrično preverjanje oz. ugotavljanje identitete nujno potrebno in da namena, ki ga upravljavec zasleduje, ni mogoče doseči zadovoljivo tudi z drugimi načini preverjanja oz. ugotavljanja identitete, ki ne vključujejo posegov v zasebnost in dostojanstvo posameznika.

Če torej podjetje, ki želi uvesti biometrijske ukrepe, ker so ti nujno potrebni za opravljanje dejavnosti, varnost ljudi ali premoženja, varovanje tajnih podatkov ali varovanje poslovne skrivnosti, za dosego teh namenov nujno potrebuje tudi biometrijsko evidentiranje delovnega časa in uspe dokazati, da so biometrijski ukrepi ne samo potrebni, temveč da so nujno potrebni in, da zasledovanega namena ni mogoče doseči na drug način, ki je s stališča zasebnosti in dostojanstva zaposlenih manj škodljiv oziroma vsiljiv, potem se tudi evidentiranje delovnega časa lahko izvede z biometrijskimi ukrepi. Praksa pa kaže, da upravljavci uvajajo biometrijske ukrepe za evidentiranje delovnega časa zgolj zato, ker je takšen način bodisi bolj praktičen od sistema z brezkontaktnimi karticami ali pa želijo preprečiti zlorabe s posojanjem kartic, pri čemer slednji razlog zgolj pavšalno navedejo in ne ponudijo tudi dovolj dokazov, da je biometrijsko evidentiranje delovnega časa nujno potrebno za opravljanje dejavnosti, varnost ljudi ali premoženja, varovanje tajnih podatkov ali varovanje poslovne skrivnosti. Zgolj navajanje razlogov za uvedbo biometrije, brez ustrezne utemeljitve, podprte z dokazi, ne zadosti zakonskim pogojem.

Na spletni strani Informacijskega pooblaščenca so objavljene povezave do odločb tujih nadzornih organov za varstvo osebnih podatkov v zvezi z uvajanjem biometrijskih ukrepov na delovnem mestu.

Ali lahko uvedete biometrijske ukrepe nad osebami, ki niso zaposlene v vašem podjetju?

Zakon je glede tega jasen. Biometrijske ukrepe v zasebnem sektorju lahko upravljavec izvaja ***zgolj*** nad svojimi zaposlenimi (prvi odstavek 80. člena ZVOP-1). Ker v pravu varstva osebnih podatkov velja načelo, da je prepovedano vse, kar z zakonom ni izrecno dovoljeno, navedeni člen daje podlago zgolj za zaposlene, kar pomeni, da nad ostalimi osebami izvajanje biometrijskih ukrepov ni dovoljeno.

Zaposlene osebe so osebe, ki so z upravljavcem sklenili pogodbo o zaposlitvi, torej le tiste osebe, ki so v delovnem razmerju z upravljavcem. Med zaposlene osebe se ne štejejo delavci, ki opravljajo občasna dela preko študentskega servisa ali na podlagi avtorske ali drugih pogodb.

Ali so odločbe Informacijskega pooblaščenca, ki jih izdaja v postopkih odločanja o izvajanju biometrijskih ukrepov, javno dostopne?

Pooblaščenec na svoji spletni strani objavlja odločbe v postopku odločanja o izvajanju biometrijskih ukrepov (izberite vsebinsko področje *biometrija*).

Zakaj so biometrijski ukrepi v zasebnem sektorju podvrženi presoji Informacijskega pooblaščenca? Ali ne gre za še eno birokratsko oviro in neupravičeno omejevanje zasebnega sektorja?

Zavedati se je potrebno, da biometrija ni le metoda ugotavljanja oz. preverjanja identitete, temveč je tehnologija, ki za svoj cilj uporablja človeško telo oziroma tiste telesne in vedenjske značilnosti vseh nas, ki so nespremenljive in samo nam lastne. Predvsem pri proizvajalcih in prodajalcih biometričnih sistemov obstaja zelo močna tendenca po trivializaciji zbiranja podatkov o človeških telesnih in vedenjskih značilnosti. Če pustimo ob strani vprašanja, ki so povezana s temeljno človekovo pravico do telesne celovitosti in dostojanstva, ima nekritična in nekontrolirana uporaba biometrije lahko zelo realne in resne posledice za vsakega posameznika. Naša zasebnost je lahko resno ogrožena zaradi nepotrebnega ali neavtoriziranega zbiranja, uporabe, neprimernega shranjevanja, povezovanja ali posredovanja naših osebnih podatkov. Četudi proizvajalci zatrjujejo, da do zlorab praktično ne more priti, pa nas zgodovina vedno znova opominja, da noben sitem ni nezlomljiv. Zakaj bi bili biometrijski sistemi izjema?

Proizvajalci biometričnih sistemov zatrjujejo, da njihovi sistemi shranjujejo predloge (*template*), t. j. reducirane, digitalizirane oblike biometričnih značilnosti, na takšen način, da rekonstrukcija izvirnih podatkov ni več mogoča. Trdijo, da unikatne značilnosti o npr. prstnem odtisu sistem zajame, jih obdela in pretovori v predlogo, na podlagi katere ni več mogoče ugotoviti, kateri osebi pripada. To utemeljujejo s tem, da so izvirni biometrični podatki zaščiteni z njihovim lastnim algoritmom, ki onemogoča rekonstrukcijo biometričnih značilnosti. Takšna trditev pa je s stališča informacijske varnosti vprašljiva vsaj iz dveh vidikov.

Prvi vidik je povezan z vprašanjem, ali je rekonstrukcija biometričnih značilnosti iz predloge mogoča oziroma, ali je mogoče razvozlati (razbiti) algoritem, ki je biometrične podatke »zakodiral«. Če poiščemo vzporednice v kriptografskih algoritmih, so praviloma najbolj varni algoritmi tisti, ki so izpostavljeni javni presoji in so na voljo vsakomur, ki jih poskuša razbiti z vsemi sredstvi, ki so mu na voljo. Za algoritem ali metodo lahko rečemo, da je varna le, če so strokovnjaki lahko preizkusili njeno nezlomljivost in ugotovili, da se brez izjemno velikih sredstev ali časa tega ne da narediti z obstoječo tehnologijo. Algoritmi in postopki lastniške ali skrite narave takšni presoji niso podvrženi in je zato težko soditi, kako varni in nezlomljivi dejansko so. Varstvo osebnih podatkov ne more temeljiti na tajnosti algoritmov ali nedostopnosti strojne opreme. Varnostni mehanizmi v tem pri-

meru predpostavljajo nevednost napadalcev, kar je pa na današnji stopnji razvoja iluzorno pričakovati. Več o možnosti rekonstrukcije izvirnih biometričnih podatkov najdete v članku Manfreda Brombe: *On the reconstruction of biometric raw data from template data*, ki je dosegljiv na naslovu: http://www.bromba.com/knowhow/temppriv.htm.

Drug vidik pa je povezan z vprašanjem, ali je preprečitev rekonstrukcije izvirnih biometričnih podatkov res odločilna pri zagotavljanju zasebnosti posameznikov in je podrobneje predstavljen v odgovoru na vprašanje št. 10. Državni nadzorni organi za varstvo osebnih podatkov se vse prepogosto srečujejo s primeri, ko se osebni podatki prvotno zbirajo z enim namenom, a se kasneje uporabljajo za povsem druge. Druga zelo pomembna izkušnja državnih nadzornih organov je, da večina posameznikov ne ceni svoje zasebnosti, dokler ni kompromitirana. In ko se to zgodi, mora posameznik znova in znova vlagati napore, da zasebnost ohranja. Težko bi trdili, da je uporaba biometričnih podatkov na to kakorkoli imuna.

Biometrija ima še eno pomembno omejitev, ki izvira iz njene narave. Biometrijske značilnosti namreč niso ključi, saj nimajo osnovnih značilnosti, ki jih imajo ključi. Za razliko od gesel ali digitalnih potrdil, biometrijske značilnosti niso skrite, se jih ne da spremeniti, uničiti ali proglasiti za neveljavne (predstavljate si lahko prstni odtis kot plastičen primer). Ključi pa so lahko skriti, lahko dobimo nove, lahko jih uničimo, spremenimo, onemogočimo, novega prstnega odtisa pa ne moremo enostavno preklicati in izdati novega. Prav tako velja eno osnovnih načel varnosti, **da ne uporabljamo istega ključa za vse** in uporabljamo različne ključe za avto, za hišo, pisarno, garažo in tako naprej. Tveganje odtujitve ali zlorabe takšnega ključa je namreč preveliko. Če si sedaj predstavljamo, da ne-kega dne vse stvari »odklepamo« z biometrijsko značilnostjo, recimo s prstnim odtisom, potem smo v isti situaciji, kot bi imeli en ključ za vse s pomembno razliko, da ne moramo »zamenjati ključavnice« oziroma še manj vseh ključavnic. Problem lahko pojasnimo še na en način. Biometrija namreč v osnovi ni tako imenovani sistem izziva in odgovora (angl. *challenge and response system*). Poenostavljano povedano, odgovor na vprašanje: »Kakšen je prstni odtis tvojega desnega kazalca?« je namreč vedno enak. Sistem izziva in odgovora pa vsakič vpraša drugačno vprašanje in je sposoben vsakič preveriti pravilnost odgovora (pomislite npr. na generatorje enkratnih gesel, ki se ponekod uporabljajo v spletnem bančništvu).

Biometrija ima svoje prednosti, vendar ima tudi svoje omejitve, katerih se je potrebno zavedati in priznavati. Vprašanja varstva osebnih podatkov pri uporabi biometrije so dovolj zgovorno pojasnjena tudi v tej prezentaciji.

Če biometrijo presojamo zgolj z vidika varstva zasebnosti, lahko torej rečemo, da biometrija ni ne grožnja zasebnosti ne njen varuh, natanko tako, kot to velja za vse druge tehnologije. Odločilna je uporaba tehnologije. Biometrija namreč lahko služi tudi večanju varstva zasebnosti, če je seveda izvedena v skladu s temeljnimi načeli in pravili varstva osebnih podatkov (načelo sorazmernosti, transparentnosti, namenskosti, ustreznem zavarovanju podatkov itd.). Prav zato Direktiva 95/46/ES v 20. členu omogoča, da je pred uvedbo določenih ukrepov potrebno pridobiti dovoljenje državnega nadzornega organa za varstvo osebnih podatkov. Slovenski zakonodajalec se je odločil, da takšno predhodno preverjanje odredi za izvajanje biometrijskih ukrepov. Informacijski pooblaščenec mora zato celovito presoditi, ali je uvajanje biometrijskih ukrepov v skladu s temi načeli in pravili varstva osebnih podatkov. Pri presoji uporabe posamezne tehnologije Pooblaščenec poleg namena, ki ga zasleduje upravljavec osebnih podatkov, tehta tudi določene tehnične lastnosti nameravanih biometrijskih ukrepov, predvsem tiste, ki nakazujejo **stopnjo tveganja uporabe določene biometrijske tehnologije**, kot so **odkritost/prikritost, puščanje sledov, možnosti povezovanja, možnost nadzora nad svojimi osebnimi podatki, (de-)centralizirano hrambo** in drugo.

Ali je potrebno pridobiti dovoljenje tudi za uporabo npr. biometričnih ključavnic v zasebni hiši, računalniku, GSM aparatu?

Ker obdelava osebnih podatkov za domače potrebe ne predstavlja rizika s stališča zasebnosti posameznika, je zakonodajalec v 7. členu ZVOP-1 predvidel generalno izjemo, ki določa, da se določbe ZVOP-1 ne uporabljajo za obdelavo osebnih podatkov, ki jo izvajajo posamezniki izključno za osebno uporabo, družinsko življenje ali za druge domače potrebe. Biometrične ključavnice na domačih vratih, računalniku ali na drugih napravah, ki se uporabljajo za osebno uporabo, vključujejo tiste načine obdelave osebnih podatkov, za katere ZVOP-1 ne velja in posledično za njihovo izvajanje ni potrebno pridobiti dovoljenja Informacijskega pooblaščenca.

Poleg tega tovrstne naprave shranjujejo biometrične podatke na takšen način, da ni razvidno kateri osebi pripadajo oziroma, jih shranjujejo tako, da se načeloma ne vzpostavlja zbirka osebnih podatkov. Tudi zaradi tega razloga ZVOP-1 v teh primerih ne pride v poštev in posledično za takšno uporabo ni potrebno dovoljenje Informacijskega pooblaščenca.

Zaposleni se strinjajo z uvedbo biometrije, imamo njihove podpisane izjave. Ali je tudi v teh primerih potrebno pridobiti dovoljenje Informacijskega pooblaščenca?

Drugi odstavek 80. člena ZVOP-1 določa, da v primeru, ko izvajanje biometrijskih ukrepov v zasebnem sektorju ni urejeno v zakonu, je upravljavec osebnih podatkov, ki namerava izvajati biometrijske ukrepe, dolžan pred uvedbo ukrepov posredovati državnemu nadzornemu organu opis nameravanih ukrepov in razloge za njihovo uvedbo. Četrti odstavek istega člena nadalje določa, da sme upravljavec osebnih podatkov izvajati biometrijske ukrepe po prejemu odločbe državnega nadzornega organa, s katero je izvajanje biometrijskih ukrepov dovoljeno. Določeno je še, da se biometrijski ukrepi lahko izvajajo nad zaposlenimi, če so bili predhodno o tem pisno obveščeni (prvi odstavek 80. člena).

Iz navedenega torej izhaja, da soglasje zaposlenih ne zadostuje za zakonito izvajanje biometrijskih ukrepov. Gre namreč za potrebni, ne pa za zadostni pogoj. Izvajanje biometrijskih ukrepov je dovoljeno le, če tako določa zakon ali če državni nadzorni organ – Informacijski pooblaščenec, z odločbo dovoli izvajanje biometrijskih ukrepov.

Kam moramo nasloviti zahtevo za dovoljenje za uvedbo biometrijskih ukrepov, obstaja kakšen vzorec in ali so s tem povezani kakšni stroški?

Vzorec obrazca prijave biometrijskih ukrepov pred njihovo uvedbo se nahaja na spletni strani Pooblaščenca http://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/PRIJAVA_BIOMETRIJSKIH_UKREPOV.doc

Obrazec za prijavo biometrijskih ukrepov ni predpisan, lahko pa vam je v pomoč pri oblikovanju zahteve za izdajo dovoljenja pred uvedbo biometrijskih ukrepov. Zahtevo pošljete na naslov Informacijskega pooblaščenca, Vošnjakova 1, PP 78, 1000 Ljubljana.

Vlogo morate kolkovati oziroma plačati upravno takso po tarifnih številkah 1 in 3 Zakona o upravnih taksah (Uradni list RS, št. 42/2007, uradno prečiščeno besedilo 3; ZUT). Upravno takso lahko tudi nakažete na TRR št. 01100-1000315637 (sklic 11 ali 18 12157-7111002). Trenutna višina upravne takse tako znaša 17,73 EUR .

Kaj naj vsebuje zahteva, obstajajo kakšna priporočila glede izpolnjevanja zahteve?

Glede na zahteve ZVOP-1 je ključno, da utemeljite, zakaj je uvedba biometrijskih ukrepov v vašem primeru nujno potrebna za enega ali več taksativno naštetih namenov: opravljanje dejavnosti, varnost ljudi ali premoženja, varovanje tajnih podatkov ali varovanje poslovne skrivnosti. Po možnosti priložite listine, s katerimi dokažete, da se v prostorih, za katere predvidevate uporabo biometrijskih ukrepov, nahajajo in obdelujejo tajni podatki, npr. dovoljenja za dostop do tajnih podatkov Ministrstva za notranje zadeve. Oglejte si tudi že izdane odločbe na spletni strani Pooblaščenca.

Pooblaščenec opozarja, da je - kot je bilo že navedeno zgoraj - biometrijske ukrepe upravičeno uvesti le, če to terja nek resen in utemeljen razlog, oziroma, če je to nujno potrebno za dosego namena, ki ga zasleduje vlagatelj. Razlog za uvedbo ni utemeljen in tudi ne nujno potreben, če vlagatelj želi uvesti biometrijske ukrepe zgolj zaradi priročnosti oziroma odsotnosti skrbi nad npr. karticami, kot alternativno rešitvijo preprečitve vstopa nepooblaščenim osebam v prostor ali sodobnostjo in privlačnostjo tehnologije kot take. Biometrijske ukrepe, ki se uvajajo le zato, ker so bolj priročni od sistemov, ki temeljijo na npr. brezkontaktnih karticah, ni mogoče opredeliti kot nujno potrebnih za dosego namenov, opredeljenih v prvem odstavku 80. člena ZVOP-1.

Pooblaščenec prav tako opozarja, da mora zahtevo za izdajo dovoljenja na Pooblaščenca nasloviti potencialni uporabnik biometrije, ne pa proizvajalec ali distributer opreme. Prav tako na odločitev Pooblaščenca ne morejo vplivati standardna besedila, ki jih pripravijo prodajalci ali distributerji opreme, temveč je na uporabniku biometrijskih ukrepov, da pojasni (predvsem) namen uvedbe biometrijskih ukrepov in utemelji nujnost uvedbe teh ukrepov. Gradiva, ki jih lahko ponudijo proizvajalci in distributerji opreme, se lahko priložijo vloge in lahko pripomorejo k razlagi tehničnih značilnosti delovanja posamezne opreme, ne morejo pa nadomestiti utemeljitve namena, ki je – kot rečeno – naloga vlagatelja zahteve, torej potencialnega uporabnika in upravljavca biometrijske naprave.

Priložiti morate ustrezen dokaz o tem, da so bili zaposleni obveščeni o nameravani uvedbi biometrijskih ukrepov (npr. datirano in ožigosano obvestilo zaposlenim ali dokument s podpisi zaposlenih). Če imate reprezentativni sindikat , v obrazec vpišite naslov reprezentativnega sindikata (sindikatov, če jih je več), ki

naj ga Pooblaščenec obvesti o uvedbi biometrije. Če tega v vašem primeru ni, potem to izrecno navedite.

Po prejemu teh informacij - oziroma povedano v pravnem jeziku – ko je vloga popolna, Informacijski pooblaščenec v roku 2 mesecev odloči, ali je nameravana uvedba biometrijskih ukrepov dovoljena.

Ali gre za obdelavo osebnih podatkov tudi, če se ne hrani slika prstnega odtisa, temveč kodirani vzorec po postopku, ki je enosmeren in ne omogoča rekonstrukcije prstnega odtisa?

Proizvajalci biometrijskih naprav se pogosto sklicujejo na trditve, da je zasebnost uporabnikov zagotovljena že s tem, ko iz predloge ni možna restavracija npr. prstnega odtisa. Predpostavimo za trenutek, da to drži. Predpostavimo, da rekonstrukcija izvirnih podatkov resnično ni možna. Četudi je to res, pa zasebnost uporabnika vseeno še ni zagotovljena, saj sta **tako vzorec prstnega odtisa kot njegov vzorec v digitalni obliki enolična identifikatorja in tako nadomeščata identiteto posameznika**. Predstavljajmo si scenarij, ko bi namesto predložitve našega biometrijskega podatka sistem deloval na podlagi npr. dvakratnika naše EMŠO. Tudi dvakratnik naše EMŠO je naš osebni podatek, čeprav ne znamo rekonstruirati originalnega podatka, ker ne vemo, kako je bil pretvorjen. Vprašanje razbitja algoritma in rekonstrukcije izvirnih podatkov je irelevantno, ne glede na to, ali se uporablja zelo enostaven algoritem (dvakratnik nekega števila) ali sofisticirano matematično metodo. Ključna vprašanja s stališča zasebnosti posameznika so povezana z uporabo, povezljivostjo in varnostjo tovrstnega identifikatorja. Napadalec bi isti namen lažje dosegel s pridobitvijo latentnega prstnega odtisa (npr. na kozarcu), kot z vlaganjem velikega napora, sredstev, znanja in časa v razbitje algoritma in s tem pridobitve izvirnih podatkov.

Kar velja za biometrične značilnosti kot take, velja tudi za digitalen zapis teh značilnosti, ki so sestavljeni na podlagi unikatnih značilnosti, ne glede na to, kolikokrat in kako je ta zapis kasneje spremenjen. Ne glede na obliko, način zapisa ali drugo spremembo, ostane vedno tista edinstvena vez z osebo, četudi se morebiti količina podrobnosti v postopku transformacije zmanjšuje (*At face value: on biometrical identification and privacy, Registratiekamer*, September 1999, str. 36).

Na podlagi tega lahko rečemo, da so biometrični podatki, četudi shranjeni v reducirani, digitalizirani obliki, vedno osebni podatki, saj se nanašajo na določeno ali vsaj določljivo osebo.

Zaključek

Odločitev glede regulacije in dopustnosti uvedbe biometrijskih ukrepov je skladno z določbami Direktive 95/46/ES lahko prepuščena odločitvi zakonodajalca v posamezni državi. Biometrija bo neizogibno postala čedalje bolj prisotna v različnih sferah našega življenja. Pot, ki jo je ubrala Slovenija, je sicer relativno stroga, vendar je s trenutno veljavnim sistemom predhodne odobritve s strani neodvisnega državnega organa zagotovljeno, da se pred uvedbo biometrijskih ukrepov izvede tako imenovana presoja vplivov na zasebnost. V nasprotnem primeru, ko bi se biometrijski ukrepi uvajali brez obveznosti takšne presoje in pridobitve dovoljenja, bi edino varovalko za varstvo temeljne človekove pravice do zasebnosti predstavljal *post festum* inšpekcijski nadzor. Pooblaščenec je zato mnenja, da je *ex ante* presoja bolj učinkovit način z vidika varstva zasebnosti, zlasti ko gre za tehnologijo, ki se šele uveljavlja, na dolgi rok pa bo tako ali drugače potrebno pretehtati ustreznost zakonskih okvirov, ki morajo slediti tehnološkemu razvoju.