Smernice glede biometrije po ZVOP-2

Smernice Informacijskega pooblaščenca

INFORMACIJSKI
POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo odgovore na najpogosteje zastavljena vprašanja z vidika zahtev novega Zakona o varstvu osebnih podatkov (ZVOP-2) glede uvedbe biometrijskih ukrepov, kot so: pod kakšnimi pogoji so biometrijski pogoji dopustni, ali gre pri tem za obdelavo osebnih podatkov, kdaj je treba in kako pridobiti dovoljenje Informacijskega pooblaščenca in druga.
Ciljne javnosti:	Subjekti javnega in zasebnega sektorja, ki razmišljajo o uvedbi biometrijskih ukrepov.
Status:	Javno
Verzija:	2.0
Datum izdaje:	26. 1. 2023
Avtorji:	Informacijski pooblaščenec; vir slik: Unsplash, Flaticon.
Ključne besede:	Smernice, biometrija, javni sektor, zasebni sektor, biometrijska značilnost, prstni odtisi, odločba, evidentiranje delovnega časa in prisotnosti na delovnem mestu, nadzor dostopa, ZVOP-2.

KAZALO

O smernicah Informacijskega pooblaščenca (IP)

Namen smernic Informacijskega pooblaščenca je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasen, razumljiv in uporaben način ter s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk osebnih podatkov. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam zakonodaje o varstvu osebnih podatkov.

Pravno podlago za izdajo smernic Informacijskemu pooblaščencu daje 3(b) odstavek 58. člena Splošne Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov; GDPR), ki določa, da ima vsak nadzorni organ pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi, med drugim, da na lastno pobudo ali na zahtevo izdaja mnenja za nacionalni parlament, vlado države članice ali, v skladu s pravom države članice, druge institucije in telesa, pa tudi za javnost, o vseh vprašanjih v zvezi z varstvom osebnih podatkov.

Oglejte si tudi:

- Mnenja IP: https://www.ip-rs.si/mnenja-gdpr/
- Brošure IP: https://www.ip-rs.si/publikacije/prirocniki-in-smernice/

Smernice IP so objavljene na spletni strani:

https://www.ip-rs.si/publikacije/prirocniki-in-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 iz Splošne uredbe in ZVOP-2, 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 novo zakonsko ureditev teh ukrepov po ZVOP-2 ter podati odgovore na najpogosteje zastavljena vprašanja s katerimi se srečujejo subjekti javnega in zasebnega sektorja, ki razmišljajo o uvedbi biometrije.

Splošno o biometriji

1. *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.

2. *Katere človeške značilnosti se v biometriji najpogosteje uporabljajo?*

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

Telesne značilnosti	Vedenjske značilnosti
• prstni odtis, • dlan, • podoba obraza, • šarenica, • očesna mrežnica • uho, • preplet ven na roki, • vonj, • DNK.	• lastnoročno podpisovanje, • govor (glas), • gibanje, • tipkanje.

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.

3. 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.

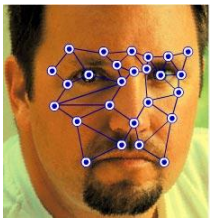
Animirani prikaz principov delovanja biometrijskih naprav si lahko ogledate na tej spletni strani:

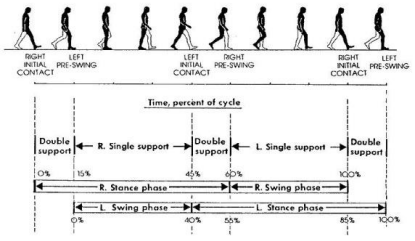
http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/default.stm.

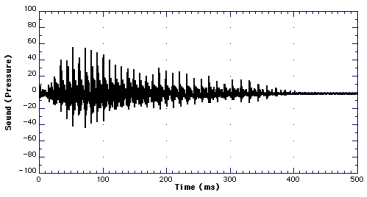
ZVOP-2 pod pojmom »biometrija« zajema dva različna načina (postopka) prepoznave biometrijskih značilnosti posameznika:

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 oziroma biometrija. 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.

Priporočamo vam tudi opis najpogostejših zmot v povezavi z biometrijo, ki ga je pripravil španski nadzorni organa za varstvo osebnih podatkov (AEPD, 2020), dostopne so (v angleškem jeziku) na:

https://www.aepd.es/es/documento/nota-equivocos-biometria-en.pdf.

4. 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 in
- posamezniku jih je težko spremeniti ali skriti.

5. Kako je biometrija urejena pri nas?

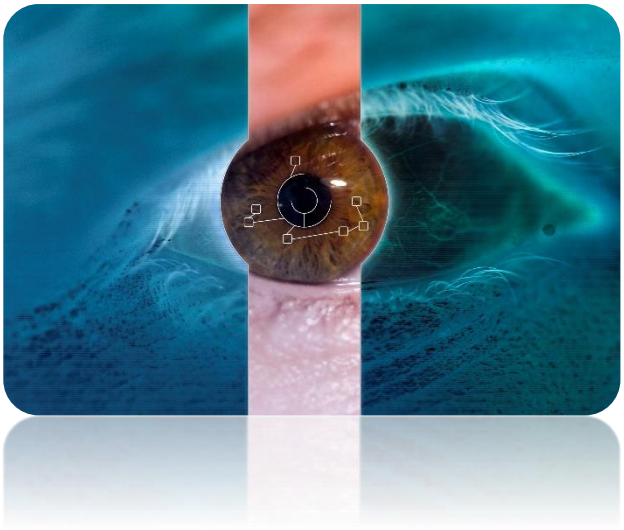
Splošna uredba v uvodni izjavi št. 53 in v četrtem odstavku 9. člena določa, da imajo države članice možnost, da ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genskih podatkov, biometričnih podatkov ali podatkov o zdravstvenem stanju. Biometrijske ukrepe ureja **Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22; ZVOP-2),** ki je nadomestil prejšnji Zakon o varstvu osebnih podatkov (ZVOP-1, Uradni list RS, št. 94/07 - uradno prečiščeno besedilo), ki je z dnem 26. 1. 2023 prenehal veljati. **ZVOP-2 ureja biometrijske ukrepe v členih od 81 do 84 (4. poglavje II. dela zakona).** Obdelava biometričnih osebnih podatkov v nasprotju z določbami tega poglavja ZVOP-2 je prepovedana. Upoštevati velja tudi določbo

desetega odstavka 80. člena ZVOP-2, ki določa, da je na javnih površinah prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic in sistemov, s katerimi se obdelujejo biometrični osebni podatki. Ob upoštevanju določbe prvega odstavka 76. člena ZVOP-2 lahko (le) drug zakon določi drugače.

Če drug zakon določa obdelavo biometričnih osebnih podatkov, poleg vsebin iz drugega ali tretjega odstavka 6. člena ZVOP-2 določi tudi pogoje za njeno uporabo, lahko pa uporabo biometričnih osebnih podatkov tudi omeji (drugi odstavek 81. člena ZVOP-2).

Prepovedano je **povezovati zbirke biometričnih osebnih podatkov z drugimi zbirkami in omogočati prenosljivost teh podatkov** v skladu z 20. členom Splošne uredbe, razen če to določa drug zakon ali v to privoli posameznik, na katerega se biometrični osebni podatki nanašajo (tretji odstavek 81. člena ZVOP-2).

Biometrija v zasebnem sektorju



Obdelava biometričnih osebnih podatkov v zasebnem sektorju se lahko izvaja le v skladu z določbami 83. člena ZVOP-2, **če je to nujno potrebno za opravljanje dejavnosti, za varnost ljudi, varnost premoženja, varovanje tajnih podatkov ali varovanje poslovnih skrivnosti**. Dejanja obdelave biometričnih osebnih podatkov morajo biti potrjena v skladu z 52. členom ZVOP-2 (prvi odstavek 83. člena ZVOP-2).

Oseba zasebnega sektorja lahko obdeluje biometrične osebne podatke tudi **zaradi varstva točnosti identitete svojih strank**. Taka obdelava je dopustna, če to za namene varovanja interesov iz prejšnjega odstavka določa drug zakon, če to posebej določa pogodba ali so stranke dale izrecno privolitev. Kadar se biometrični osebni podatki obdelujejo na podlagi pogodbe s potrošnikom, mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, omogočiti tudi način identifikacije brez obdelave biometričnih osebnih podatkov.

Obdelava biometričnih osebnih podatkov v zasebnem sektorju se sme izvajati **tudi pod pogojem, da so dejanja obdelave teh podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo ter potrjena** v skladu s pristojnostmi nadzornega organa za potrjevanje iz 52. člena ZVOP-2 in omogoča stranki, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete (odstavek 83. člena ZVOP-2).

Pred začetkom obdelave biometričnih osebnih podatkov morajo biti **posamezniki o tem pisno obveščeni**, kadar gre za zaposlene, pa mora upravljavec z zaposlenimi izvesti predhodno posvetovanje o sorazmernosti obdelave (.četrti odstavek 83. člena ZVOP-2).

Po določbi petega odstavka 83. člena ZVOP-2 **oseba zasebnega sektorja**, ki namerava obdelovati biometrične osebne podatke, **pred začetkom obdelave posreduje nadzornemu organu opis nameravanih obdelav in razloge za njihovo uvedbo** (glejte Obrazec za prijavo biometrijskih ukrepov Informacijskemu pooblaščencu). Informacijski pooblaščenec po prejemu potrebnih informacij v dveh mesecih odloči, ali je biometrija dovoljena v skladu z določbami ZVOP-2. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca. Upravljavec osebnih podatkov sme izvajati biometrijske ukrepe

šele **po prejemu odločbe Informacijskega pooblaščenca**, s katero je izvajanje biometrijskih ukrepov dovoljeno. Zoper odločbo Informacijskega pooblaščenca ni pritožbe, dovoljen pa je upravni spor.

*Za Izvajanje biometrijskih ukrepov brez pozitivne odločbe Pooblaščenca je zagrožena globa od **2.000** do **10.000 EUR** za pravno osebo oz. če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, od **4.000** do **20.000 eurov**; globa od **500** do **4.000 EUR** grozi tudi odgovorni osebi.*

ZVOP-2 določa tudi **možno izjemo**
in sicer osebi zasebnega sektorja ni treba pridobiti odločbe, če se biometrični ukrepi izvajajo na način iz tretjega odstavka 83. člena ZVOP-2, t.j. so **dejanja obdelave teh podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo ter potrjena** v skladu s pristojnostmi nadzornega organa za potrjevanje iz 52. člena ZVOP-2 in **omogoča stranki, da izrecno dovoli obdelavo** teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

Ob tem velja izpostaviti, da 121. člen ZVOP-2 v prehodnih določbah glede potrjevanja določa, da Slovenska akreditacija začne izvajati postopke akreditacije 1. januarja 2024, da pa se do začetka izvajanja postopkov akreditacije po tem zakonu šteje, da so dejanja obdelave upravljavcev in obdelovalcev, ki morajo po določbah tega zakona za dejanja obdelave pridobiti certifikat, ta skladna z merili iz mehanizma potrjevanja. Upravljavci vloge za potrjevanje in vloge po drugem stavku prvega odstavka 83. člena tega zakona vložijo v roku šestih mesecev po poteku roka iz prvega odstavka tega člena. Obdelave, za katere je bila v roku iz prejšnjega stavka dana vloga za akreditacijo, se štejejo za skladne z merili iz mehanizma potrjevanja do 31. decembra 2024.

ZVOP-2 v 84. členu opredeljuje **prepoved pridobivanja biometričnih osebnih podatkov v zvezi s trženjem** in sicer določa, da se v okviru trženja ali podobne druge poslovne dejavnosti ne smejo zahtevati, pridobiti ali nadalje obdelovati biometrični osebni podatki v zamenjavo za določene storitve, četudi so te storitve za posameznika, na katerega se nanašajo osebni podatki, brezplačne.

Biometrija v javnem sektorju

ZVOP-2 v 82. členu določa, da se obdelava biometričnih osebnih podatkov v javnem sektorju lahko **določi le z zakonom**, **če je to nujno potrebno za varnost ljudi, varnost premoženja ali za varovanje tajnih podatkov, za identifikacijo pogrešanih ali umrlih posameznikov ali za varovanje poslovnih skrivnosti, teh namenov pa ni mogoče doseči z milejšimi sredstvi**.

Obdelavo biometričnih osebnih podatkov v javnem sektorju je **izjemoma** dopustno izvajati tudi **pod pogojem, da so dejanja obdelave teh podatkov potrjena** v skladu s pristojnostmi nadzornega organa za potrjevanje iz 52. člena ZVOP-2 na način, ki zagotavlja obdelavo in uporabo teh podatkov posameznika pod njegovim izključnim nadzorom ali izključno oblastjo ter mu omogoča, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete (drugi odstavek 82. člena ZVOP-2).

Ne glede na prvi odstavek 82. člena ZVOP-2 se obdelave biometričnih osebnih podatkov lahko določi z zakonom, če gre za **izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja** (tretji odstavek 82. člena ZVOP-2).

Obdelava biometričnih osebnih podatkov v javnem sektorju se lahk**o določi z zakonom tudi za namen identifikacije posameznikov pri izdaji sredstev elektronske identifikac**ije v skladu z zakonom, ki ureja

sredstva elektronske identifikacije, in če je tako identifikacijo posameznik zahteval (četrti odstavek 82. člena ZVOP-2).

V javnem sektorju se lahko z drugim zakonom **izjemoma** uvede obdelava biometričnih osebnih podatkov **v zvezi z vstopom v stavbo ali dele stavbe**, ki se izvedejo ob smiselni uporabi četrtega, petega in šestega odstavka 83. člena tega zakona, če je to nujno potrebno za varnost ljudi, varnost premoženja, varovanje tajnih podatkov ali varovanje poslovnih skrivnosti. (peti odstavek 82. člena ZVOP-2). Slednje pomeni, da je za te namene potrebno pridobiti odločbo Informacijskega pooblaščenca, posamezniki morajo biti o tem pisno obveščeni, kadar gre za zaposlene, pa mora upravljavec z zaposlenimi izvesti predhodno posvetovanje o sorazmernosti obdelave.

6. Zakaj je področje biometrije urejeno v Zakonu o varstvu osebnih podatkov (ZVOP-2)?

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-2.

7. Katere so ključne razlike med ureditvijo biometrije po ZVOP-1 in ZVOP-2?

Ključne razlike so naslednje:

- Obdelava biometričnih osebnih podatkov v javnem sektorju se lahko določi z zakonom tudi, če je to nujno potrebno za identifikacijo pogrešanih ali umrlih posameznikov, tega namena pa ni mogoče doseči z milejšimi sredstvi.
- Obdelava biometričnih osebnih podatkov v javnem sektorju se lahko določi z zakonom tudi za namen identifikacije posameznikov pri izdaji sredstev elektronske identifikacije v skladu z zakonom, ki ureja sredstva elektronske identifikacije, in če je tako identifikacijo posameznik zahteval.
- ZVOP-2 **ne omejuje več uporabe biometrije v zasebnem sektorju samo nad zaposlenimi**, temveč je pod določenimi pogoji mogoče biometrijo uporabljati tudi **nad strankami** (npr. zaradi varovanja točnosti identitete strank).

- Delodajalec se ni več dolžan posvetovati z **reprezentativnim sindikatom**, mora pa opraviti **posvetovanje z zaposlenimi** glede sorazmernosti obdelave.
- **Pod določenimi pogoji pridobitev predhodnega dovoljenja (odločbe) Informacijskega pooblaščenca ni več obvezna** (glej deveti in tretji odstavek 83. člena ZVOP-2).
- Izrecno je **na javnih površinah prepovedana uporaba sistemov, s katerimi se obdelujejo biometrični osebni podatki** (npr. prepoznava obrazov posameznikov na ulicah; glej deseti odstavek 80. člena ZVOP-2).
- Razen ob določenih izjemah je **prepovedano povezovati zbirke biometričnih osebnih podatkov z drugimi zbirkami in omogočati prenosljivost teh podatkov** tretji odstavek 81. člena ZVOP-2).
- **Prepovedano je pridobivanje biometričnih osebnih podatkov v zvezi s trženjem** - v okviru trženja ali podobne druge poslovne dejavnosti se ne smejo zahtevati, pridobiti ali nadalje obdelovati biometrični osebni podatki v zamenjavo za določene storitve, četudi so te storitve za posameznika brezplačne.

8. *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[1].

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.

9. *Ali se biometrične značilnosti vedno štejejo za posebne vrste osebne podatke?*

V uvodni izjavi št. 51 Splošne uredbe je izpostavljeno, da si posebno varstvo zaslužijo osebni podatki, ki so po svoji naravi posebej občutljivi z vidika temeljnih pravic in svoboščin, saj bi lahko okoliščine njihove obdelave resno ogrozile temeljne pravice in svoboščine. Obdelava fotografij se ne bi smela sistematično šteti za obdelavo posebnih vrst osebnih podatkov, saj spadajo v opredelitev biometričnih podatkov le, kadar

[1] At face value: on biometrical identification and privacy, Registratiekamer, September 1999, str. 36

so **obdelane s posebnimi tehničnimi sredstvi, ki omogočajo edinstveno identifikacijo ali avtentikacijo posameznika.**

Po določbi 14. točke 4. člena Splošne uredbe izraz »biometrični podatki“ pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki. Splošna uredba nima posebne definicije posebnih vrst osebnih podatkov, temveč 9. člen Splošne uredbe glede obdelave posebnih vrst osebnih podatkov določa, da sta prepovedani obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

10. 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 bili dovoljeni. V tem primeru bi podjetje kršilo temeljno načelo, zapisano v (b) točki prvega odstavka 5. člena Splošne uredbe, ki določa, da se osebni podatki ne smejo nadalje obdelovati na način, ki ni združljiv 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.

***

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

1. 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 . 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 odločbe 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:

Morda bi izpostavili 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).

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

2. Ali se lahko v podjetju uvede biometrijo za evidentiranje delovnega časa zaposlenih?

Po določbi 83. člena ZVOP-2 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 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. Izjema je določa za javni sektor in sicer se v javnem sektorju lahko z drugim zakonom izjemoma uvede obdelava biometričnih osebnih podatkov v zvezi z vstopom v stavbo ali dele stavbe, ki se izvedejo ob smiselni uporabi četrtega, petega in šestega odstavka 83. člena tega zakona, če je to nujno potrebno za varnost ljudi, varnost premoženja, varovanje tajnih podatkov ali varovanje poslovnih skrivnosti. (peti odstavek 82. člena ZVOP-2). Slednje pomeni, da je za te namene potrebno pridobiti odločbo Informacijskega pooblaščenca, posamezniki morajo biti o tem pisno obveščeni, kadar gre za zaposlene, pa mora upravljavec z zaposlenimi izvesti predhodno posvetovanje o sorazmernosti obdelave.

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 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 pogojem iz zakona.

3. *Ali se lahko uvede biometrijske ukrepe nad osebami, ki niso zaposlene v vašem podjetju?*

ZVOP-2 je glede je glede tega v primerjavi z ZVOP-1 bolj odprt in tovrstne izrecne omejitve ne vsebuje več, ob določenih pogojih je mogoče biometrijske ukrepe uporabljati tudi nad strankami - glejte pogoje za uvedbo biometrijskih ukrepov, kot so opisani zgoraj.

4. *Ali moramo pridobiti novo odločbo po ZVOP-2, če smo jo že pridobili po ZVOP-1?*

ZVOP-2 ne vsebuje prehodnih določb, ki bi nakazovale, da že izdane odločbe pred uveljavitvijo ZVOP-2 (torej po ZVOP-1) niso več veljavne, zato obstoječe odločbe ostajajo veljavne in upravljavcem ni treba pridobiti novih odločb.

5. *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 primeru 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 nekega 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 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.). Splošna uredba v uvodni izjavi št. 53 in v četrtem odstavku 9. člena določa, da imajo države članice možnost, da ohranijo ali uvedejo dodatne pogoje, tudi

omejitve, glede obdelave genskih podatkov, biometričnih podatkov ali podatkov o zdravstvenem stanju. 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 Informacijski pooblaščenec tehta poleg namena, ki ga zasleduje upravljavec osebnih podatkov, 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.

Poudariti velja tudi, da nimajo vse biometrijske tehnologije enakih implikacij na zasebnost – prepoznava obrazov posameznikov na javnih površinah vsekakor predstavlja občutnejši poseg kot prepoznava prstnih odtisov pri vstopu v sistemsko sobo posameznega upravljavca. **Zlasti prepoznava obrazov na javnih površinah se v zadnjem času kaže kot zelo nevarna za posege v celo vrsto temeljnih pravic in svoboščin (glej npr. skupno izjavo Evropskega nadzornika za varstvo podatkov in Evropskega odbora za varstvo podatkov** – »Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov pozivata k prepovedi uporabe umetne inteligence za avtomatizirano prepoznavanje človekovih značilnosti v javno dostopnih prostorih in nekaterih drugih načinov uporabe umetne inteligence«, dostopno na: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_sl ter smernice Evropskega odbora o prepoznavi obrazov, dostopno na: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf).

6. *Ali je treba pridobiti dovoljenje tudi za uporabo npr. biometričnih ključavnic v zasebni hiši, računalniku, na mobilnem aparatu?*

Ker obdelava osebnih podatkov za domače potrebe ne predstavlja takšnih tveganj s stališča zasebnosti posameznika, je zakonodajalec v 3. členu ZVOP-2 predvidel generalno izjemo, ki določa, da se določbe ZVOP-2 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-2 ne velja, in posledično za njihovo izvajanje ni potrebno pridobiti dovoljenja Informacijskega pooblaščenca.

Stanje pa je lahko drugačno, če ne gre za samostojno odločitev posameznika, da bo za vstop v službeni računalnik ali odklepanje mobilnega telefona uporabi prstni odtis ali prepoznavo obrazca, temveč za odločitev delodajalca, da npr. za vstop v delovne naprave, sisteme ali aplikacije zahteva uporabo biometrijskih podatkov (npr. prepoznavo prstnega odtisa) – v tem primeru pa gre za klasično uporabo biometrije, za katero veljajo določbe ZVOP-2.

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

Po določbi petega odstavka 83. člena ZVOP-2 **oseba zasebnega sektorja**, ki namerava obdelovati biometrične osebne podatke, **pred začetkom obdelave posreduje nadzornemu organu opis nameravanih obdelav in razloge za njihovo uvedbo** (glejte Obrazec za prijavo biometrijskih ukrepov Informacijskemu

pooblaščencu). Informacijski pooblaščenec po prejemu potrebnih informacij v dveh mesecih odloči, ali je biometrija dovoljena v skladu z določbami ZVOP-2. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca. Upravljavec osebnih podatkov sme izvajati biometrijske ukrepe šele **po prejemu odločbe Informacijskega pooblaščenca**, s katero je izvajanje biometrijskih ukrepov dovoljeno. Zoper odločbo Informacijskega pooblaščenca ni pritožbe, dovoljen pa je upravni spor.

Pred začetkom obdelave biometričnih osebnih podatkov morajo biti posamezniki o tem pisno obveščeni, kadar gre za zaposlene, pa mora upravljavec z zaposlenimi izvesti predhodno posvetovanje o sorazmernosti obdelave (četrti odstavek 83. člena ZVOP-2). 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.

8. *Kam je treba 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 Informacijskega 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. Obrazec je posodobljen glede na določbe ZVOP-2.

Zahtevo pošljete na naslov Informacijskega pooblaščenca, Dunajska 22, 1000 Ljubljana ali na elektronski naslov gp.ip@ip-rs.si.

Vlogo morate kolkovati oziroma plačati upravno takso po tarifnih številkah 1 in 3 Zakona o upravnih taksah (Uradni list RS št 106/10 – UPB 5), ki skupaj znese 22,60 EUR. Upravno takso najlažje plačate z nakazilom na TRR št. 01100-1000315637, s sklicem na 11 ali 18 12157-7111002. Potrdilo o nakazilu priložite vlogi ali ga posredujete kasneje, do izdaje odločbe.[2]

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

Glede na zahteve ZVOP-2 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 Informacijskega pooblaščenca.

[2] Višina upravne takse je odvisna od trenutne vrednosti točke, zato se lahko s časom spreminja. Izračun je zato vezan na dan izdaje teh smernic.

Informacijski 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 83. člena ZVOP-2.

Informacijski pooblaščenec prav tako opozarja, da mora zahtevo za izdajo dovoljenja na Informacijskega pooblaščenca nasloviti potencialni uporabnik biometrije, ne pa proizvajalec ali distributer opreme. Prav tako na odločitev Informacijskega 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.

Če se bodo biometrijski ukrepi izvajali nad zaposlenimi, morate priložiti 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 ter **dokazilo o posvetovanju z zaposlenimi glede sorazmernosti obdelave** (priložite npr. zapisnik o posvetovanju).

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. Zoper odločbo Informacijskega pooblaščenca ni pritožbe, dovoljen pa je upravni spor.

10. Kdaj so »dejanja obdelave biometričnih podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo«?

ZVOP-2 v tretjem odstavku 83. člena določa, da se sme obdelava biometričnih osebnih podatkov v zasebnem sektorju izvajati tudi pod pogojem, da so dejanja **obdelave teh podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo** ter potrjena v skladu s pristojnostmi nadzornega organa za potrjevanje iz 52. člena ZVOP-2 in omogoča stranki, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

Iz obrazložitve predloga ZVOP-2 ni razbrati dodatnih pojasnil, vendar pa je treba tendenco zakonodajalca razumeti v smislu spodbujanja načela **vgrajenega in privzetega varstva osebnih podatkov**[3] (25. člen Splošne uredbe). Skladno s tem načelom se skrbi za to, da se zakonite cilje dosega na način, ki kar najmanj posega v zasebnost posameznikov – eden od takšnih prijemov je tudi izogibanje centralizirani hrambi osebnih podatkov in uveljavljanj močnejšega nadzora posameznika nad lastnimi osebnimi podatki, kot npr. na način, da se biometrijski podatki ne hranijo v centraliziranih zbirkah in sistemih pri upravljavcu ali obdelovalcu,

[3] Glej npr. Information and Privacy Commissioner for Canada: Privacy by Design; dostopno na: https://www.ipc.on.ca/wp-content/uploads/Resources/PrivacybyDesignBook.pdf (str. 109)

temveč na medijih ali napravah, ki so pod nadzorom posameznika (npr. mobilni telefon, osebni računalnik, USB ključki in podobni mediji). V takšnih primerih se lahko preverjanje biometrijskih značilnosti izvede na sami napravi posameznika in se upravljavcu sploh ne posredujejo biometrični podatki, temveč zgolj rezultat preverjanja (npr. »gre za pravo osebo/ne gre za pravo osebo«) in se ji posledično dovoli dostop do določenih sistemov oziroma se tako preveri/potrdi njena identiteta. Pri tem upravljavec ne zbere in ne shrani posameznikovih biometrijskih podatkov, temveč zgolj rezultat preverjanja, ki se kot rečeno izvede »pod izključnim nadzorom ali izključno oblastjo« posameznika. ZVOP-2 za takšne primere implementacije biometrije omogoča določene olajševalne okoliščine za zavezance, zlasti v luči tega, da **v tem primeru ni treba pridobiti predhodne pozitivne odločbe** Informacijskega pooblaščenca (.deveti odstavek 83. člena ZVOP-2) – navedeno velja zgolj za zasebni sektor.

11. 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 Splošne uredbe 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, se je pa uporaba biometrije zlasti v zasebnem sektorju nekoliko prilagodila tehnološki realnosti. S sistemom predhodne odobritve neodvisnega državnega organa – če podlaga za uporabo biometrije ni določena za zakonom, je zagotovljeno, da se pred uvedbo biometrijskih ukrepov izvede presoja nujnosti uporabe biometrije skladno z zakonskimi omejitvami. 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. Informacijski 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 – kot je bilo to storjeno z ZVOP-2 – potrebno ponovno pretehtati ustreznost zakonskih okvirov, ki morajo slediti tehnološkemu razvoju.