

BIOMETRIJA IN VARSTVO OSEBNIH PODATKOV: KAKO NA TEHNOLOGIJO GLEDA ZAKONODAJA?

ANA ANTUNIČEVIĆ

Consilium ius d.o.o., Ljubljana, Slovenija
ana@consilium.si

V tem prispevku se avtorica osredotoča na vzpostavitev nove zakonodaje s področja varstva osebnih podatkov tako na ravni Evropske Unije (GDPR) kot tudi na ravni Slovenije (ZVOP-2) in njen vpliv na obdelavo osebnih podatkov v okviru biometrične tehnologije.

DOI
[https://doi.org/
10.18690/um.feri.1.2024.1](https://doi.org/10.18690/um.feri.1.2024.1)

ISBN
978-961-286-837-6

Ključne besede:
varstvo osebnih podatkov,
zakonodaja,
GDPR,
ZVOP-2,
biometrija



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.feri.1.2024.1](https://doi.org/10.18690/um.feri.1.2024.1)

ISBN
978-961-286-837-6

Keywords:
personal data protection,
legislation,
GDPR,
ZVOP-2,
biometrics

BIOMETRICS AND PERSONAL DATA PROTECTION: LEGAL PERSPECTIVE

ANA ANTUNIČEVIĆ

Consilium ius d.o.o., Ljubljana, Slovenia
ana@consilium.si

In this paper, the author focuses on the establishment of new legislation in the field of personal data protection both at the European Union level (GDPR) and at the Slovenian level (ZVOP-2) and its impact on the processing of personal data in the context of biometric technology.



1 Uvod

V današnjem času na praktično vseh področjih beležimo hiter razvoj digitalizacije. Ti tehnološki preboji odpirajo vrata novim načinom komunikacije, poslovanja, obdelave in shranjevanja množice podatkov, ki je bila mnogoterim še pred kratkim nepredstavljiva. Vendar pa ta digitalna revolucija prinaša tudi nove izzive; eden takšnih je tudi varovanje zasebnosti in varstvo osebnih podatkov.

Kot odgovor na večje spremembe v družbi, se je pojavila zakonodaja, ki do določene mere ureja uporabo tehnologije ter določa varnostne mehanizme, s katerimi se dviguje nivo varstva zasebnosti. Razvoj zakonodaje v takšnih trenutkih je ključen, tako z vidika zagotavljanja varnosti kot tudi razvoja tehnologije, ki jo zakonodaja ureja. Pri pripravi takšne zakonodaje pa je pomembno, da je fleksibilna in dovolj odprta, saj se mora prilagajati spreminjajočim se potrebam in tehnološkim inovacijam. Hkrati pa se je potrebno zavedati dejstva, da zakonodaja vedno nastaja kot odgovor na nastale razmere, kar neizogibno vodi v dejstvo, da po sprejemu in vpeljavi takšne zakonodaje, velikokrat dobimo občutek, da je »zastarela« še preden smo jo sploh uporabili. Okoliščine še dodatno otežuje zares bliskovit razvoj tehnologije, ki smo mu priča v zadnjem času.

V takšnih okoliščinah je nastala Splošna uredba o varstvu osebnih podatkov¹ (v nadaljevanju tudi samo GDPR), s katero je Evropska Unija poskusila uokviriti obdelavo osebnih podatkov. Čeprav morda GDPR na prvi vtis deluje predvsem na področju spleta in z njim povezanih velikanov kot sta Google in Meta, pa lahko ob bolj podrobnem pregledu, hitro ugotovimo, da ureditev obdelave osebnih podatkov, ki jo določa GDPR, posega tudi v poslovne procese in razvoj ter uporabo določenih tehnologij, kamor sodi tudi biometrija, o kateri bomo govorili v tem prispevku.

¹ UREDBA (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). Dostopno na: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679>.

2 Pogled na obdelavo osebnih podatkov skozi določila GDPR in slovenskega Zakona o varstvu osebnih podatkov

2.1 Sprejem GDPR in Zakona o varstvu osebnih podatkov

Evropska unija je leta 2016 sprejela Splošno uredbo o varstvu osebnih podatkov² (GDPR), ki je nadomestila do sedaj veljavno Direktivo 95/94/ES. Po sprejemu GDPR je nastopil 2 letni *vacatio legis*³, ki je omogočal državam članicam kot tudi zavezancem in upravičencem po GDPR, čas, da se seznanijo z novo zakonodajo in jo ustrezno implementirajo. Po poteku tega obdobja, je GDPR stopila v veljavo, kar se je zgodilo 25.5.2018.

Na tej točki je pomembno poudariti, da je GDPR Uredba EU, kar pomeni, da gre za zavezujoč pravni akt, ki velja **neposredno v vseh državah članicah EU**, brez da bi bil potreben kakršenkoli prenos s sprejemom nacionalne zakonodaje. Ravno neposredna uporabljivost pa je ključna razlika med Uredbo EU (kot je GDPR) in Direktivo EU (kot je bila Direktiva 95/46/ES, ki jo nadomešča GDPR). Direktiva EU namreč določa cilje oz. začrta smernice, ki se jih morajo države članice držati, vendar pa jo mora vsaka država članica **prenesti v svoj nacionalni pravni red**. Upoštevajoč zgoraj napisano direktiva prinese manj poenoteno zakonodajo na ravni EU, saj imajo države članice pri prenosu direktive več maneverskega prostora, medtem ko pri Uredi EU **vsebinsko odstopanje ni mogoče** – države članice se morajo v celoti ravnati skladno z besedilom uredbe; ločeno pa lahko obravnavajo določene tematike, ki niso del uredbe ali pa določene tematike obravnavajo bolj ali manj rigorozno kot specifična uredba (vendar znotraj meja, ki jih začrta uredba).

Sprejem GDPR je bil torej velik preskok za Evropsko Unijo, saj je določila s področja varstva osebnih podatkov do sedaj urejala direktiva, medtem ko ima GDPR status Uredbe in s tem močno dviguje **unifikacijo prava držav članic EU na področju varstva osebnih podatkov in zasebnosti**.

² Kot zgoraj.

³ Gre za obdobje, ki sledi sprejetju zakona (in objavi v uradnem glasilu), vendar pred uveljavitvijo zakona. To obdobje zavezancem, ki jih zakon zavezuje omogoča, da se prilagodijo na izvajanje nove zakonodaje (npr. sprejmejo nove ukrepe, prilagodijo poslovne procese ipd.).

Po sprejemu, vendar zlasti po **uveljavitvi GDPR** je sledila evforija urejanja skladnosti z GDPR v slovenskem gospodarskem prostoru. Vendar se je začetna evforija, ki so jo spremljale predvsem ogromne količine e-sporočil tipa »ostanite z nami«, kmalu polegla. GDPR pa je bila v Sloveniji razglašena za brezzobega tigra.

Kaj točno se je zgodilo?

Da bi razumeli, zakaj je GDPR v Sloveniji »obvisela v zraku« in zakaj ni bilo mogoče izreči nobene globe, si je potrebno pogledati razliko med materialnim in procesnim zakonom.

Medtem ko materialni zakon določa pravice in obveznosti v zvezi z določeno vsebino (oz. materijo), kot je npr. varstvo osebnih podatkov, pa procesni zakon ureja postopke in načine izvrševanja materialnih zakonov. Če povedano apliciramo na naš primer: GDPR je sama po sebi materialni predpis (zakon oz. uredba), zato za svojo polno uveljavitev potrebuje procesni zakon, ki ga Slovenija vse do leta 2023 ni sprejela.

S sprejemom Zakona o varstvu osebnih podatkov⁴ (v nadaljevanju tudi samo ZVOP-2) je Slovenija dobila procesni del kot tudi nekatere materialne dopolnitve, ki podrobneje opredeljujejo določila GDPR. Eno izmed takšnih področij je tudi področje biometrije, o katerem bomo pisali v tem prispevku.

2.2 Osnove varstva osebnih podatkov po GDPR in ZVOP-2

Preden se spustimo v podrobno obravnavo biometrije in biometričnih osebnih podatkov, se je potrebno seznaniti z osnovami varstva osebnih podatkov po veljavni zakonodaji.

Ključen pojem, ki nikakor ni tako enoznačen kot zveni, je namreč **osebni podatek**. GDPR določa, da osebni podatek: *»pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni*

⁴ Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika»⁵.

Hitro vidimo, da je definicija **splošna in predvsem zelo široka**. Če jo na kratko povzamemo, lahko zaključimo, da je osebni podatek katerakoli informacija (ali sklop informacij), na podlagi katere je posameznik **določljiv**. Ne gre torej za standard **določenosti**; tj. da je posameznik v celoti identificiran (tipičen primer določenosti je npr. kombinacija imena, priimeka in naslova, ki velikokrat privedejo do določenosti posameznika), temveč **določljivosti**, kar pomeni, da na skupek različnih informacij **določi posameznika**.

Informacijski pooblaščenec je v svoji infografiki pripravil določene tipske kategorije osebnih podatkov, in sicer osebne podatke uvršča v naslednje kategorije:

- **Identifikacijski podatki** (ime in priimek, EMŠO, davčna številka, IP naslov ipd.),
- **Kontaktne podatki** (telefonska številka, e-mail, naslov ipd.),
- **Transakcijski podatki** (podatki o nakupih, zdravstvenih storitvah, podatki o uporabi spleta, lokacijski podatki ipd.) in
- **Statusni podatki** (podatki o zdravju, premoženju, željah, preferencah, izobrazbi, spolu, poklicu ipd.).⁶

Prav tako je zelo širok pojem **obdelave osebnih podatkov**, ki po GDPR vključuje katerakoli operacijo na osebnih podatkih, kot so: hramba, posredovanje, spreminjanje, uničenje in izbris.⁷

⁵ Člen 4, I. odstavek, UREDBA (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. Dostopno na: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679>

⁶ Povzeto po Infografiki Informacijskega pooblaščenca, ki je dostopna na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Infografika%20-%20osebni%20podatki2.pdf

⁷ Člen 4, II. odstavek, UREDBA (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. Dostopno na: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679>

2.3 Zakonitost obdelave osebnih podatkov

Na podlagi GDPR je obdelava osebnih podatkov zakonita, kadar poteka na **ustrezni pravni podlagi** in za vnaprej opredeljen, jasno določen, zakonit in javno objavljen **namen**.

Pravne podlage, na katerih je možna obdelava osebnih podatkov, so določene v 6. členu GDPR in so taksativno naštet, kar pomeni, da smo dolžni pravno podlago izbrati v okviru tega člena.

GDPR določa naslednje pravne podlage:

- Zakon,
- Soglasje,
- Pogodbena razmerje,
- Zaščita življenjskih interesov,
- Zaščita javnega interesa (izvajanje javne oblasti) in
- Zakoniti interesi.⁸

Preden se v praksi izvede obdelavo osebnih podatkov, je torej potrebno opredeliti: (1) zakaj bomo to obdelavo izvajali (**namen obdelave**) in (2) na kateri pravni podlagi se bo takšna obdelava izvajala (**določitev pravne podlage**).

Pri sami izvedbi je potrebno paziti še na obveznost informiranja posameznikov (13. in 14. člen GDPR) in spoštovanje načel GDPR (5. člen GDPR), kjer je potrebno izpostaviti zlasti načelo transparentnosti in načelo minimizacije podatkov; slednje je ključno pri določanju obsega osebnih podatkov, ki jih potrebujemo, da dosežemo namen, ki smo si ga zadali.

3 Ureditev biometrije v Sloveniji

V tem prispevku se bomo osredotočili na ureditev obdelave biometričnih osebnih podatkov, skladno z ZVOP-2, ki velja v Sloveniji.

⁸ Člen 6, UREDBA (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). Dostopno na: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679>.

Področje biometrije, v okviru GDPR velja za posebnost, saj GDPR v 9. členu določa, da smejo države članice uvesti dodatne pogoje in omejitve, kadar gre za obdelavo biometričnih podatkov⁹. Kot odgovor na to določilo, se je slovenski zakonodajalec odločil za bolj podrobno opredelitev obdelave biometričnih podatkov znotraj ZVOP-2, ki si jo bomo pogledali v tem delu prispevka.

Ločeni ureditvi biometrije je posvečeno 4. poglavje ZVOP-2 z naslovom »Obdelava osebnih podatkov z uporabo biometrije in genskih podatkov«¹⁰. Preden pa se posvetimo vsebini poglavja, je potrebno določiti kaj biometrija sploh je in zakaj jo obravnavamo v okviru varstva osebnih podatkov.

3.1 O biometriji

»Biometrija je eden izmed načinov ugotavljanja oz. preverjanja identitete«, povzame definicijo biometrije Informacijski pooblaščenec in nadaljuje, da gre pri biometriji za preverjanje identitete na podlagi neke vedenjske oz. telesne značilnosti, ki je lastna samo tej osebi¹¹. Pri biometričnih sistemih ločimo verifikacijo in identifikacijo.

Pri verifikaciji gre za sistem preverja ali je oseba zares tista, za katero se izdaja. Gre torej za preverbo biometričnega vzorca z vzorcem, ki se nahaja v bazi.¹² Pri identifikaciji pa gre za prepoznavo posameznika, na podlagi podatkovne baze, ki je v sistemu.¹³

Ne glede na to ali gre za verifikacijo ali identifikacijo pa za obdelavo osebnih podatkov potrebujemo biometrične značilnosti, kot so: obraz, prstni odtis, DNA, očesna mrežnica, hoja, glas in drugi¹⁴. Te biometrične značilnosti predstavljajo tudi biometrične osebne podatke, kadar govorimo o obdelavi osebnih podatkov.

⁹ Člen 9, IV. Odstavek, UREDBA (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). Dostopno na: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679>.

¹⁰ 4. poglavje, ¹⁰ Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

¹¹ Povzeto po: <https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/prijava-biometrijskih-ukrepov/>.

¹² MATJAŠEC, Matjaž, 2018, Metode biometričnega overjanja: sistematičen pregled literature [na spletu]. Magistrsko delo. Maribor: Univerza v Mariboru. [Dostopano 19 februar 2024]. Pridobljeno s: <https://dk.um.si/IzpisGradiva.php?lang=slv&id=70945>, stran 6.

¹³ Kot zgoraj.

¹⁴ MATJAŠEC, Matjaž, 2018, Metode biometričnega overjanja: sistematičen pregled literature [na spletu]. Magistrsko delo. Maribor: Univerza v Mariboru. [Dostopano 19 februar 2024]. Pridobljeno s: <https://dk.um.si/IzpisGradiva.php?lang=slv&id=70945>, stran 8.

Kljub temu, da biometrične značilnosti temeljijo na unikatnih značilnostih, ki so vezane na posameznika, pa je potrebno opozoriti, da biometrija ni 100% natančna, saj se pri delovanju zanaša na določeno mero verjetnosti (medtem ko na drugi strani uporaba gesla zagotavlja 100% učinkovitost, saj je geslo lahko le pravilno ali napačno – ne more pa biti npr. pravilno s 96% verjetnostjo).¹⁵

Preden se torej odločimo za uporabo biometričnih ukrepov, je torej smiselno, da dobro premislimo, ali je tak ukrep res najprimernejši.

3.2 Ureditev biometrije v ZVOP-2

Tako kot je bilo predstavljeno zgoraj, se tudi ZVOP-2 opira na dva načina prepoznave biometrijskih značilnosti in sicer na **identifikacijo** in **avtentikacijo**. ZVOP-2 ureja biometrične ukrepe v členih 81 – 84 pri čemer v 81. členu najdemo splošne prepovedi, kot npr. prepoved povezovanja zbirk biometričnih osebnih podatkov z drugimi zbirkami¹⁶. V nadaljevanju pa ZVOP-2 predpisuje način uporabe biometričnih ukrepov, pri čemer deli uporabo biometrije na zasebni in javni sektor.

3.2.1 Biometrični osebni podatki

Ker ta prispevek temelji na biometričnih osebnih podatkih, si bomo ogledali še ali gre pri biometričnih podatkih vedno tudi za osebne podatke ali obstajajo kakšne izjeme, ko lahko biometrične podatke uporabljamo, ne da bi šlo za obdelavo osebnih podatkov.

Pogosto je v okviru uporabe biometrije omenjeno, da »ne gre za obdelavo osebnih podatkov«, saj se za prepoznavo uporabljajo zgolj »predloge« (tj. zapis vzorca v digitalni obliki) in ne izvirni osebni podatek (npr. prstni odtis).

Tako na evropski kot na slovenski ravni je sprejeto stališče, da digitalni zapis biometričnih značilnosti (t.i. »*template*« ali predloga) predstavlja **osebni podatek** na enak način kot surovi zapis biometrične značilnosti.

¹⁵ Smernice španskega nadzornega organa za varstvo osebnih podatkov; 14 misunderstandings with regard to biometric identification and authentication, dostopno na <https://www.aepd.es/documento/nota-equivocos-biometria-en.pdf>.

¹⁶ Člen 81, III. Odstavek, Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

Takšno stališče je sprejeto na podlagi (zgoraj opredeljenega) koncepta osebnega podatka. Videli smo, da je neka informacija osebni podatek, kadar je na podlagi te informacije posameznik **določljiv** (in ne nujno določen). Prav tako smo v tem prispevku pisali, da je namen biometrije **prepoznavna posameznika** glede na njegove distinktivne značilnosti. Upoštevajoč navedeno, bo obdelava podatkov z biometričnimi podatki **vedno predstavljala obdelavo osebnih podatkov**, saj je njihov **prvotni namen** prepoznavna (in s tem tudi določljivost) posameznika. Glede na navedeno, je potrebno za uporabo biometrije spoštovati določila GDPR in ZVOP-2.

3.2.2 Ureditev v zasebnem sektorju

Uporabo v **zasebnem sektorju** določa 83. člen, ki pravi, da je obdelava biometričnih podatkov dovoljena le, *»kadar je to **nujno potrebno** za opravljanje dejavnosti, za varnost ljudi, varnost premoženja, varovanje tajnih podatkov ali varovanje poslovnih skrivnosti»*¹⁷.

Dodatno je v zasebnem sektorju uporaba **biometrije** dopustna tudi *»zaradi varstva točnosti identitete svojih strank»*¹⁸. Tudi v tem primeru zakon določa omejitve, na podlagi katerih je takšna raba mogoča, kadar je to nujno potrebno zaradi opravljanja dejavnost oz. varnosti (kot opredeljeno zgoraj), kadar takšno obdelavo posebej določa pogodba ali pa kadar je bila pridobljena privolitev stranke.

Zgornja dva odstavka opredeljujeta **pravno podlago** in **namene obdelave**, ki jih je potrebno določiti pri uporabi biometrije.

Kot vidimo, je nabor pravnih podlag ozek, saj ZVOP-2 določa, da je obdelava biometričnih osebnih podatkov dovoljena samo na podlagi zakona. Nekoliko širši nabor je zgolj v primeru, da gre za točnost identitete **strank**, kjer lahko upravljavec osebnih podatkov izbira med pravnimi podlagami: zakon, pogodbeno razmerje in privolitev posamične stranke.

¹⁷ Člen 83, I. odstavek, Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

¹⁸ Člen 83, II. odstavek, Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

Prav tako je **ozek in vnaprej opredeljen** tudi nabor namenov obdelave, ki jim lahko služijo biometrični ukrepi; kot je to razvidno iz zgornjih odstavkov, gre za namene: varovanja (ljudi, premoženja) ali pa varstva točnosti identitete stranke.

V zasebnem sektorju je omogočena tudi raba biometričnih ukrepov, skladno s 3. odstavkom, 83. člena ZVOP-2. V tem primeru gre za **izjemo**, ki omogoča uporabo biometričnih osebnih podatkov za druge namene, v kolikor takšna obdelava poteka **pod izključnim nadzorom stranke** ali **pod njeno izključno oblastjo** in omogoča stranki, da izrecno dovoli obdelavo teh podatkov. Prav tako mora biti takšna obdelava **potrjena** s strani nadzornega organa za potrjevanje, o čemer bomo pisali v ločenem poglavju.

Najbolj zanimiva pojma v zgornjem odstavku sta gotovo »izključni nadzor« in »izključna oblast«, ki ju bo morala napolniti pravna praksa. Do sedaj pa se lahko opremo na mnenje Informacijskega pooblaščenca, ki pravi, da bo potrebno oba pojma razlagati »v smislu spodbujanja načela vgrajenega in privzetega varstva osebnih podatkov¹⁹«, ki ga uvaja GDPR.

Zgornje načelo je potrebno razlagati na način, da je potrebno za doseg ciljev upoštevati metode, ki čim manj posegajo v zasebnost posameznika in spodbujajo visok nivo varstva osebnih podatkov. Informacijski pooblaščenec navaja, da je eden takih ukrepov tudi »*preprečitev hrambe podatkov v centraliziranih zbirkah pri upravljavcu, temveč omogočanje hrambe na medijih ali napravah, ki so pod nadzorom posameznika (npr. mobilni telefon, USB ključki ipd.)*²⁰«.

V primeru, da se upravljavec odloči za tak pristop, mu za vpeljavo **ni potrebno** pridobiti pozitivne odločbe Informacijskega pooblaščenca (opis tega postopka se nahaja spodaj), kar nekoliko olajša postopek sprejemanja biometričnih ukrepov v organizaciji.

¹⁹ Mnenje Informacijskega pooblaščenca; št. 07121-1/2024/128, z dne 5.2.2024, dostopno na: <https://www.ip-rs.si/mnenja-zvop-2/potrjevanje-obdelav-biometri%C4%8Dnih-op-1707898494>.

²⁰ Kot zgoraj.

3.2.3 Postopek uvedbe biometrije v zasebnem sektorju

Postopek, kako se uvede biometrične ukrepe, je prav tako opredeljen v ZVOP-2, in sicer od 4. do 8. odstavka 83. člena. Upravljavalec je dolžan še pred začetkom obdelave biometričnih osebnih podatkov o tem obvestiti zaposlene in z zaposlenimi izvesti predhodno posvetovanje o sorazmernosti obdelave.

Naslednji korak je posredovanje opisa nameravanih obdelav in razlogov za uvedbo Informacijskemu pooblaščenca. Pri Informacijskem pooblaščenca so pripravili obrazec, ki ga lahko uporabijo upravljavci. Po prejemu vseh informacij, bo Informacijski pooblaščenec **v roku 2 mesecev** odločil o dovoljenosti uporabe biometrije. Upravljavalec sme vpeljati biometrične ukrepe šele **po prejemu pozitivne odločbe s strani Informacijskega pooblaščenca**.

3.2.4 Biometrija v javnem sektorju

Podobno kot v zasebnem sektorju se tudi biometrija v javnem sektorju lahko določi z zakonom, in sicer »če je to nujno potrebno za varnost ljudi, varnost premoženja, varovanje tajnih podatkov, identifikacijo pogrešanih ali umrlih posameznikov ali za varovanje poslovnih skrivnosti, teh namenov pa ni mogoče doseči z milejšimi sredstvi«²¹.

Prav tako je v javnem sektorju omogočena tudi izjema, ki dopušča obdelavo biometričnih osebnih podatkov, »kadar so dejanja obdelave akreditirana in kadar se obdelava izvaja pod izključnim nadzorom ali izključno oblastjo posameznika ter mu omogoča, da izrecno dovoli obdelavo teh podatkov«²².

Prav tako ZVOP-2 določa nekaj dodatnih izjem, ki pa so namenjene izpolnjevanju mednarodnih obveznosti ali pa identifikaciji v okviru postopka izdaje sredstev elektronske identifikacije.

²¹ Člen 82, I. odstavek, Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

²² Člen 82, II. odstavek, Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

3.3 Akreditacija

Kot je bilo že omenjeno v zgornjih poglavjih, je kot pogoj za uporabo biometrije omenjena tudi akreditacija posamične biometrijske rešitve. Skladno z ZVOP-2 bi morala slovenska akreditacija pričeti z delovanjem 1.1.2024, vendar do danes akreditacija še ni bila vzpostavljena. Vprašanja, kot so: katero telo bo skrbelo za akreditacijo, kakšen bo postopek in nenazadnje tudi kakšna bo cena takšne akreditacije, tako v času priprave tega prispevka ostajajo neodgovorjena.

V vmesnem obdobju pa se je pri uporabi biometričnih rešitev potrebno opreti na 2. odstavek 121. člena, ki vzpostavlja domnevo, da so vsa »dejanja obdelave upravljavcev in obdelovalcev, ki morajo po določbah tega zakona za dejanja obdelave pridobiti certifikat, ta skladna z merili iz mehanizma potrjevanja«²³.

4 Zaključno

Obdelava osebnih podatkov postaja čedalje bolj kompleksna tema, kjer je prisotno vsakodnevno tehtanje med zmožnostjo tehnologije in posegom v zasebnost posameznika. GDPR, kot temeljni predpis s področja varstva osebnih podatkov, postavlja pravni okvir, znotraj katerega morajo upravljavci in obdelovalci vzpostaviti ustrezne mehanizme in varovalke, ki bodo omogočali varno obdelavo osebnih podatkov.

V tem prispevku je bila podrobneje predstavljena tudi ureditev biometrije v slovenski zakonodaji. V tem primeru je Slovenija specifična v primerjavi z drugimi državami članicami, naša ureditev pa močno odstopa tudi od ureditve GDPR, ki specifičnih določb o biometriji nima.

Čeprav je v primerjavi s prejšnjim (in sedaj neveljavnim) Zakonom o varstvu podatkov (ZVOP-1), sedaj uporaba biometrije širša, še posebej za zasebni sektor, pa lahko trdimo, da je manevrski prostor za biometrične rešitve v slovenskem prostoru relativno ozek.

²³ Člen 121, II. Odstavek, Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>.

Na tej točki je potrebno izpostaviti izjemo, ki jo omogoča ZVOP-2, kjer se lahko upravljavci, ki želijo uporabiti biometrijo, izognejo potrjevanju takšne rešitve pri Informacijskem pooblaščenca, v kolikor jim uspe zagotoviti, da so vsa dejanja obdelave osebnih podatkov pod izključnim nadzorom ali izključno oblastjo posameznika, čigar podatke se obdeluje. Tukaj v ospredje prihajata dve načeli, ki ju je vzpostavila GDPR, in sicer t.i. »privacy by design« in »privacy by default«, ki naj upravljavcem služita kot smernici pri vzpostavitvi biometričnih ukrepov brez odločbe Informacijskega pooblaščenca.

Svoj košček v biometričnem mozaiku pa bo dodala tudi akreditacija, ki bo določala, kako široko se bodo odprla vrata za uporabo biometrije in nenazadnje tudi kako visok bo prag (tako z vidika tehnologije kot tudi z vidika stroškov postopka akreditacije), ki ga bo potrebno prestopiti za rabo takšne tehnologije.

V luči povedanega torej lahko zaključimo, da ostaja uporaba biometrije v Sloveniji visoko regulirana, vendar pa je, v primerjavi s prej veljavnim zakonom, prišlo do vidnih premikov k dostopnosti tovrstne tehnologije.

Viri in literatura

- UREDBA (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. Dostopno na: <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679>;
- Zakon o varstvu osebnih podatkov, UL RS; št. 003-02-22024-4. Dostopno na: <https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187?sop=2022-01-4187>;
- Infografika Informacijskega pooblaščenca, ki je dostopna na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Infografika%20-%20osebni%20podatki2.pdf;
- MATJAŠEC, Matjaž, 2018, Metode biometričnega overjanja: sistematičen pregled literature [na spletu]. Magistrsko delo. Maribor: Univerza v Mariboru. [Dostopano 19 februar 2024]. Pridobljeno s: <https://dk.um.si/IzpisGradiva.php?lang=slv&cid=70945>;
- Smernice španskega nadzornega organa za varstvo osebnih podatkov; 14 misunderstandings with regard to biometric identification and authentication, dostopno na: <https://www.aepd.es/documento/nota-equivocos-biometria-en.pdf>.
- Mnenje Informacijskega pooblaščenca; št. 07121-1/2024/128, z dne 5.2.2024, dostopno na: <https://www.ip-rs.si/mnenja-zvop-2/potrjevanje-obdelav-biometri%C4%8Dnih-op-1707898494>.