Mnenje odbora (člen 64)

Mnenje 11/2024 o uporabi tehnologij za prepoznavanje obrazov za pospešitev pretoka letaliških potnikov (skladnost s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov)

Različica 1.1

sprejeto 23. maja 2024

Sprejeto

Različica 1.1	28. maj 2024	Slovnični popravek v povzetku (strani 3 in 4) ter točkah 77 in 90 mnenja
Različica 1.0	23. maj 2024	sprejetje mnenja

Povzetek

Francoski nadzorni organ je pri Evropskem odboru za varstvo podatkov (EOVP) zahteval izdajo mnenja o uporabi tehnologije za prepoznavanje obrazov, ki jo upravljavci letališč in letalske družbe uporabljajo za biometrično avtentikacijo ali identifikacijo potnikov, da bi se pospešil pretok potnikov na letališčih.

EOVP uvodoma opozarja, da uporaba biometričnih podatkov in zlasti tehnologije za prepoznavanje obrazov pomeni večja tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki (v nadaljevanju: posamezniki). Nanaša se na obdelavo biometričnih podatkov, ki se jim v skladu z 9. členom Splošne uredbe o varstvu podatkov zagotavlja posebno varstvo. Upravljavci bi morali pred uporabo takih tehnologij, tudi če bi se štele za posebej učinkovite, oceniti, kakšen je njihov učinek na temeljne pravice in svoboščine posameznikov ter preučiti, ali se lahko njihov zakoniti namen obdelave doseže z manj vsiljivimi sredstvi.

Področje uporabe tega mnenja je v skladu z zahtevkom omejeno na to, ali je obdelava združljiva s **točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov** za **posebni namen pospešitve pretoka potnikov na letališčih** na štirih posameznih kontrolnih točkah, in sicer na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice. To mnenje ne zajema popolne in celovite analize tega, ali zadevni upravljavci in njihovi obdelovalci, če je ustrezno, v vsakem primeru zagotavljajo skladnost s Splošno uredbo o varstvu podatkov. Zato ne posega v pravno in tehnično analizo posameznih primerov, ki temelji na predvideni posebni obdelavi in okoliščinah upravljavca. Poleg tega analiza veljavne pravne podlage ne spada v obseg vprašanj, predloženih EOVP v zahtevku, zato v tem mnenju ni preučena veljavnost privolitve v tako obdelavo v skladu s 6., 7. in 9. členom Splošne uredbe o varstvu podatkov. Poleg tega to mnenje ne posega v omejitve uporabe biometričnih podatkov, določene v zakonodaji držav članic.

EOVP v tem mnenju ocenjuje skladnost obdelave z zgoraj navedenimi določbami Splošne uredbe o varstvu podatkov v okviru **štirih posebnih scenarijev**.

Po **scenariju 1** vpisano biometrično predlogo hrani posameznik, na primer na osebni napravi, ki je pod njegovim izključnim nadzorom, in sicer za avtentikacijo potnika (primerjava „ena proti ena“) pri prehodu skozi navedene kontrolne točke na letališču.

EOVP ugotavlja, da bi se lahko štelo, da izbrani ukrepi izpolnjujejo načelo potrebnosti, če lahko upravljavec dokaže, da ni alternativnih rešitev, ki manj posegajo v zasebnost, s katerimi bi se lahko enako učinkovito dosegel isti cilj. Poleg tega se lahko poseganje v zasebnost pri obdelavi uravnoteži z dejavnim sodelovanjem potnikov, saj svojo biometrično predlogo hranijo sami, na primer na osebni napravi, ki je pod njihovim izključnim nadzorom, njihovi podatki pa se izbrišejo kmalu po tem, ko je ugotavljanje ujemanja končano. EOVP na podlagi tega ugotavlja, da **bi se lahko načeloma štelo,** da je obdelava iz prvega scenarija **združljiva s točko f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov**, če bi se izvajali ustrezni zaščitni ukrepi.

EOVP je opredelil minimalne zaščitne ukrepe, ki bi jih bilo treba izvajati vsaj pri rešitvi, podobni prvemu scenariju.

Po **scenariju 2** se vpisana biometrična predloga v šifrirani obliki centralizirano hrani na letališču, pri čemer bi imel ključ oziroma skrivni podatek le potnik. To omogoča avtentikacijo potnikov (primerjava „ena proti ena“) pri prehodu skozi navedene kontrolne točke na letališču. Vpis je veljaven za določeno

obdobje, kar je lahko na primer do enega leta po zadnjem letu ali do datuma poteka veljavnosti potnega lista.

EOVP ugotavlja, da bi se lahko štelo, da obdelava izpolnjuje načelo potrebnosti, če lahko upravljavec dokaže, da ni alternativnih rešitev, ki manj posegajo v zasebnost, s katerimi bi se lahko enako učinkovito dosegel isti cilj. Poleg tega se lahko poseganje v zasebnost pri obdelavi uravnoteži z dejavnim sodelovanjem potnika, saj ima pod izključnim nadzorom ključ oziroma skrivni podatek do svojih šifriranih biometričnih podatkov. Če bi upravljavec izvajal ustrezne zaščitne ukrepe, bi se lahko varnostna tveganja zaradi uporabe centralizirane podatkovne zbirke v tem scenariju zmanjšala, negativni vpliv na temeljne pravice in svoboščine posameznikov pa bi se lahko obravnaval kot sorazmeren s pričakovano koristjo. EOVP glede načela omejitve hrambe niso bile predložene nobene informacije, s katerimi bi se utemeljilo dolgo obdobje hrambe. Da bi se v tem scenariju dosegla skladnost s točko e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov, bi morali biti upravljavci zmožni utemeljiti, zakaj je v posebnih primerih za ta namen potrebno predvideno obdobje hrambe. EOVP priporoča, da upravljavci predvidijo najkrajše možno obdobje hrambe, hkrati pa potnikom ponudijo možnost, da določijo želeno obdobje hrambe. EOVP na podlagi tega ugotavlja, da **bi se lahko načeloma štelo**, da je obdelava iz scenarija 2 **združljiva s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov,** če bi se izvajali ustrezni zaščitni ukrepi.

EOVP je opredelil minimalne zaščitne ukrepe, ki bi jih bilo treba izvajati vsaj pri rešitvi, podobni drugemu scenariju.

Po **<u>scenariju 3</u>** se vpisana biometrična predloga v šifrirani obliki centralizirano hrani na letališču pod nadzorom upravljavca letališča. To omogoča identifikacijo potnika (primerjava „ena proti N“) pri prehodu skozi navedene kontrolne točke na letališču. Obdobje hrambe v tem scenariju je običajno 48 ur, podatki pa se izbrišejo, ko letalo vzleti.

Osebni in biometrični podatki se hranijo v osrednji podatkovni zbirki. Če bi bila ogrožena zaupnost podatkovne zbirke, bi to lahko posledično privedlo do dostopa do celotnega nabora podatkov in bi se lahko omogočila nepooblaščena ali nezakonita identifikacija potnikov v drugih okoljih. Zaradi centralizirane arhitekture za hrambo, ki je pod nadzorom upravljavca letališča, potniki tudi bolj izgubijo nadzor nad svojimi podatki. EOVP meni, da je mogoče podoben rezultat, kakršen se doseže s pospešitvijo pretoka potnikov na letališčih, doseči na način, ki manj posega v zasebnost, ter da negativni vpliv na temeljne pravice in svoboščine posameznikov, ki bi bil posledica kršitve varnosti podatkov v centralizirani podatkovni zbirki biometričnih podatkov, prevlada nad pričakovanimi koristmi, ki izhajajo iz obdelave. Zato obdelava ne more izpolnjevati načel potrebnosti in sorazmernosti. EOVP na podlagi tega ugotavlja, da obdelava iz tretjega scenarija **ne more biti združljiva s 25. členom Splošne uredbe o varstvu podatkov**. Če bi se upravljavec omejil na ukrepe, opisane v tem scenariju, to prav tako **ne bi bilo v skladu s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov**.

Po **<u>scenariju 4</u>** se vpisana biometrična predloga v šifrirani obliki centralizirano hrani v oblaku pod nadzorom letalske družbe ali njenega ponudnika storitev v oblaku. To omogoča identifikacijo potnikov (primerjava „ena proti N“) pri prehodu skozi navedene kontrolne točke na letališču. Obdobje hrambe v tem scenariju lahko traja, dokler ima stranka račun pri letalski družbi.

Identifikacijski in biometrični podatki se hranijo v osrednji podatkovni zbirki v oblaku, zato bi lahko imelo do takih podatkov dostop več subjektov, tudi morebitni ponudniki iz držav zunaj EGP. Podatki o potniku se med uporabo dešifrirajo, ključi pa so pod nadzorom letalske družbe ali njenih obdelovalcev,

kar bi lahko povečalo obseg varnostne izpostavljenosti. Zaradi take centralizirane arhitekture za hrambo potniki tudi bolj izgubijo nadzor nad svojimi podatki. Podatki bi se lahko hranili tudi daljše obdobje, zato bi bili izpostavljeni večjemu tveganju kršitve varnosti, kar bi presegalo to, kar je nujno in sorazmerno za obdelavo, razen če se sprejmejo dodatni ukrepi za zmanjšanje tveganja za posameznike.

EOVP meni, da je mogoče podoben rezultat, kakršen se doseže s pospešitvijo pretoka potnikov na letališčih, doseči na način, ki manj posega v zasebnost, ter da negativni vpliv na temeljne pravice in svoboščine posameznikov, ki bi lahko bil posledica kršitve varnosti podatkov v centralizirani podatkovni zbirki biometričnih podatkov, prevlada nad pričakovanimi koristmi, ki izhajajo iz obdelave. Zato obdelava ne more izpolnjevati načel potrebnosti in sorazmernosti. EOVP na podlagi tega ugotavlja, da obdelava iz scenarija 4 **ne more biti združljiva s 25. členom Splošne uredbe o varstvu podatkov**. Če bi se upravljavec omejil na ukrepe, opisane v tem scenariju, to na podlagi informacij, ki so na voljo EOVP, prav tako **ne bi bilo v skladu s točko e prvega odstavka 5. člena** ter **točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov**.

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju 63. člena in drugega odstavka 64. člena 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 (v nadaljevanju: **Splošna uredba o varstvu podatkov**),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju 10. in 22. člena Poslovnika (v nadaljevanju: **Poslovnik EOVP**) Evropskega odbora za varstvo podatkov (v nadaljevanju: **EOVP**),

ob upoštevanju naslednjega:

(1) Glavna naloga EOVP je zagotoviti dosledno uporabo Splošne uredbe o varstvu podatkov v celotnem Evropskem gospodarskem prostoru (**EGP**). Drugi odstavek 64. člena Splošne uredbe o varstvu podatkov določa, da lahko kateri koli nadzorni organ, predsednica EOVP ali Evropska komisija zahteva, da katero koli zadevo splošne uporabe ali z učinkom v več kot eni državi članici EGP preuči EOVP, ki da mnenje.

(2) Mnenje EOVP se v skladu s tretjim odstavkom 64. člena Splošne uredbe o varstvu podatkov v povezavi z drugim odstavkom 10. člena Poslovnika EOVP sprejme v osmih tednih po tem, ko predsednica EOVP in pristojni nadzorni organi sklenejo, da je dokument popoln. Predsednica lahko odloči, da se to obdobje glede na kompleksnost vsebine podaljša za šest tednov –

sprejel naslednje mnenje:

1 UVOD

1.1 Povzetek dejstev

1. Francoski nadzorni organ je 16. februarja 2024 pri EOVP zahteval izdajo mnenja o tem, ali je uporaba tehnologije za prepoznavanje obrazov, ki upravljavcem letališč in letalskim družbam omogoča biometrično avtentikacijo ali identifikacijo potnikov[2], združljiva s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov, da bi se pospešil pretok potnikov na varnostnih kontrolnih točkah na letališču[3], pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice (razen mejne kontrole in pregledov, ki jih opravljajo brezcarinske prodajalne) (v nadaljevanju: **zahtevek**). Francoski nadzorni organ je zahtevku priložil opis običajnih primerov uporabe (Priloga I).

[1] Sklice na „**države članice**“ v tem mnenju je treba razumeti kot sklice na „države članice EGP“. Sklice na „Unijo“ ali „EU“ v tem mnenju je treba razumeti kot sklice na „EGP“.
[2] V tem mnenju „**potnik**“ pomeni posameznika, na katerega se nanašajo osebni podatki, katerega osebni podatki se obdelujejo za poseben namen, opisan v tem mnenju. V nadaljevanju tega mnenja se izraza „potnik“ in „posameznik“ uporabljata kot sopomenki.
[3] V tem mnenju se pojem „**varnostne kontrolne točke na letališču**“ nanaša na varnostne preglede, ki se izvajajo v pristojnosti upravljavca letališča in jih morajo opraviti potniki, da lahko iz terminala za odhode vstopijo na območje ali izhod za vkrcanje.

2. Francoski nadzorni organ v zahtevku ugotavlja, da se modeli, ki se trenutno preskušajo na več letališčih EU, med državami članicami razlikujejo, kar bi lahko povzročilo tveganje, da bi bila med razlagami nadzornih organov razhajanja in da bi to različno vplivalo na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, v EU[4].

3. EOVP meni, da je treba odgovor na zahtevek podati tako, da se odgovori na naslednji vprašanji:

4. **<u>1. vprašanje</u>:**

1.1 Ali je lahko uporaba tehnologije za prepoznavanje obrazov za biometrično avtentikacijo, ki je **namenjena pospešitvi pretoka potnikov na letališčih** (na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice), združljiva s **točko f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov,** v primeru arhitekture za hrambo, v kateri biometrično predlogo vsakega potnika hrani **le posameznik**, na primer lokalno na osebni napravi pod svojim izključnim nadzorom?

1.2 Če bi bila taka obdelava združljiva z navedenimi določbami, kateri minimalni ustrezni zaščitni ukrepi bi bili potrebni ob upoštevanju 25. in 32. člena Splošne uredbe o varstvu podatkov?

<u>2. vprašanje</u>:

2.1 Ali je lahko uporaba tehnologije za prepoznavanje obrazov za biometrično avtentikacijo ali identifikacijo, ki je **namenjena pospešitvi pretoka potnikov na letališčih** (na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice), združljiva s **točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov** v primeru **centralizirane** arhitekture za hrambo, pri kateri se biometrična predloga vsakega potnika hrani v osrednji podatkovni zbirki:

2.1.1 V osrednji podatkovni zbirki na letališču pod nadzorom upravljavca letališča, v šifrirani obliki, s ključem oziroma skrivnim podatkom za avtentikacijo, ki ga pozna le posameznik (in se hrani na primer na mobilnem telefonu)?

2.1.2 Če bi bila taka obdelava združljiva, kateri minimalni ustrezni zaščitni ukrepi bi bili potrebni ob upoštevanju 25. in 32. člena Splošne uredbe o varstvu podatkov?

2.2.1 V osrednji podatkovni zbirki na letališču, ki je pod nadzorom upravljavca letališča, v šifrirani obliki s ključi za identifikacijo, ki jih pozna upravljavec letališča?

2.2.2 Če bi bila taka obdelava združljiva, kateri minimalni ustrezni zaščitni ukrepi bi bili potrebni ob upoštevanju 25. in 32. člena Splošne uredbe o varstvu podatkov?

2.3.1 V oblaku, pod nadzorom letalske družbe ali njenega ponudnika storitev (obdelovalca), v šifrirani obliki, s ključi za identifikacijo, ki jih pozna letalska družba ali njen ponudnik storitev?

[4] Zahtevek, str. 1.

2.3.2 Če bi bila taka obdelava združljiva, kateri minimalni ustrezni zaščitni ukrepi bi bili potrebni ob upoštevanju 25. in 32. člena Splošne uredbe o varstvu podatkov?

5. Potem ko je francoski nadzorni organ 16. februarja 2024 menil, da je dokument popoln, in je 23. februarja 2024 tako menila tudi predsednica EOVP, je sekretariat dokument razposlal 23. februarja 2024. Predsednica EOVP se je v skladu s tretjim odstavkom 64. člena Splošne uredbe o varstvu podatkov v povezavi z drugim odstavkom 10. člena Poslovnika EOVP odločila, da predpisan osemmesečni rok zaradi kompleksnosti zadeve podaljša še za šest tednov.

1.2 Dopustnost zahtevka za mnenje iz drugega odstavka 64. člena Splošne uredbe o varstvu podatkov

6. V drugem odstavku 64. člena Splošne uredbe o varstvu podatkov je določeno, da lahko kateri koli nadzorni organ zahteva, da katero koli zadevo splošne uporabe ali z učinkom v več kot eni državi članici preuči EOVP, ki da mnenje.

7. EOVP meni, da se zahtevek, ki ga je predložil francoski nadzorni organ v zvezi z združljivostjo uporabe tehnologije za prepoznavanje obrazov za biometrično avtentikacijo ali identifikacijo, ki je namenjena pospešitvi pretoka potnikov na letališčih, nanaša na vprašanja „z učinkom v več kot eni državi članici“, saj se na letališčih držav članic, kot je pojasnjeno v zahtevku[5], trenutno uvaja več projektov in se ocenjuje, da se bo taka uporaba v prihodnjih letih povečala. Modeli, ki jih trenutno preskušajo različna letališča in letalski prevozniki, se med državami članicami zelo razlikujejo, kar bi lahko povzročilo tveganje, da bi z vidika varstva podatkov prišlo do različnih učinkov v več kot eni državi članici.

8. Poleg tega EOVP meni, da ima zahtevek, ki ga je predložil francoski nadzorni organ, pomembne posledice za uporabo načel iz točk e in f prvega odstavka 5. člena Splošne uredbe o varstvu podatkov ter zahtev, ki se uporabljajo za upravljavce na podlagi 25. člena Splošne uredbe o varstvu podatkov, pa tudi zahtev, ki se uporabljajo za upravljavce in obdelovalce na podlagi 32. člena Splošne uredbe o varstvu podatkov. Zato se ta zahtevek nanaša na „zadevo splošne uporabe“ v smislu drugega odstavka 64. člena Splošne uredbe o varstvu podatkov, saj se nanaša na dosledno razlago načel omejitve hrambe (točka e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov), celovitosti in zaupnosti (točka f prvega odstavka 5. člena Splošne uredbe o varstvu podatkov) ter pojmov vgrajenega in privzetega varstva podatkov (25. člen Splošne uredbe o varstvu podatkov) in varnosti podatkov (32. člen Splošne uredbe o varstvu podatkov), da se med drugim zagotovi dosledna uporaba navedenih določb v EGP.

9. Morebitna različna stališča držav članic glede razlage točk e in f prvega odstavka 5. člena ter 25. in 32. člena Splošne uredbe o varstvu podatkov bi povečala tveganje, da upravljavci letališč in letalske družbe ne bi dosledno razvijali projektov prepoznavanja obrazov. Ker je francoski nadzorni organ pokazal jasno potrebo po dosledni razlagi teh določb v zvezi s tehnologijo za prepoznavanje obrazov za biometrično avtentikacijo ali identifikacijo potnikov, da bi se pospešil pretok potnikov na letališčih[6], EOVP meni, da je zahtevek utemeljen v skladu s tretjim odstavkom 10. člena Poslovnika EOVP.

10. V skladu s tretjim odstavkom 64. člena Splošne uredbe o varstvu podatkov EOVP ne izda mnenja, če je o zadevi že izdal mnenje[7]. EOVP še ni odgovoril na vprašanja, ki izhajajo iz zahtevka. Čeprav Smernice

[5] Zahtevek, str. 3.
[6] Zahtevek, str. 1–3.
[7] Tretji odstavek 64. člena Splošne uredbe o varstvu podatkov in četrti odstavek 10. člena Poslovnika EOVP.

EOVP 3/2019 o video napravah[8] že vsebujejo nekatere koristne elemente o varnostnih ukrepih, ki bi jih bilo treba uporabiti pri obdelavi biometričnih podatkov, ne obravnavajo vseh vidikov v zvezi z vprašanji iz zahtevka. Poleg tega razpoložljive smernice EOVP, vključno s Smernicami EOVP 3/2019 o video napravah, ne vsebujejo posebnih smernic o morebitnih elementih, ki jih je treba preveriti v zvezi s centralizirano ali decentralizirano hrambo biometričnih podatkov za identifikacijo ali avtentikacijo potnikov, da bi se pospešil pretok potnikov na letališčih, in o združljivosti take obdelave s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov.

11. EOVP zato meni, da je zahtevek dopusten, vprašanja, ki izhajajo iz njega, pa bi bilo treba analizirati v mnenju, sprejetem v skladu z drugim odstavkom 64. člena Splošne uredbe o varstvu podatkov.

2 PODROČJE UPORABE MNENJA IN PODLAGA ZA MNENJE

2.1 Področje uporabe mnenja

12. To mnenje se nanaša le na to, ali upravljavci letališča in letalske družbe uporabljajo tehnologijo za prepoznavanje obrazov za biometrično avtentikacijo ali identifikacijo potnikov skladno s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov **za namen pospešitve pretoka potnikov na letališčih**, in sicer na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice, kot je navedeno v zahtevku.

13. EOVP v zvezi s **področjem uporabe tega mnenja** pojasnjuje naslednje:

    1) Obdelava osebnih podatkov v okviru mejnih kontrol in pregledov, ki jih opravljajo brezcarinske prodajalne, ne spada na področje uporabe tega mnenja, saj jih opravljajo upravljavci, ki niso upravljavci letališča in letalske družbe.

    2) Uporaba tehnologije za prepoznavanje obrazov, tudi če temelji na scenarijih, opisanih v nadaljevanju v oddelku 3.2, za kateri koli drug namen (kot je preprečevanje, odkrivanje in preiskovanje kaznivih dejanj) ali s strani katere koli druge osebe, čeprav za podoben namen, ne spada na področje uporabe tega mnenja.

    3) To mnenje obravnava le obdelavo osebnih podatkov potnikov in ne zajema drugih vrst posameznikov, kot so osebje upravljavcev letališč ali letalskih družb.

    4) V tem mnenju je proučena zahteva francoskega nadzornega organa v zvezi z združljivostjo arhitektur za hrambo biometričnih predlog potnikov s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov. V zvezi s tem v mnenje ni vključena popolna in celovita analiza tega, ali zadevni upravljavci in njihovi obdelovalci, če je ustrezno, v vsakem primeru zagotavljajo skladnost s Splošno uredbo o varstvu podatkov. To je zlasti pomembno glede na to, da te tehnologije pomenijo večja tveganja, povezana z obdelavo posebnih vrst podatkov v skladu z 9. členom Splošne uredbe o varstvu podatkov. Zato to mnenje ne posega v oceno drugih določb Splošne uredbe o varstvu podatkov, kar zadeva uporabo tehnologij za prepoznavanje obrazov, tudi v posebnem sektorju, na katerega

[8] Smernice 3/2019 o obdelavi osebnih podatkov z video napravami, različica 2.0, sprejete 29. januarja 2020 (v nadaljevanju: **Smernice EOVP 3/2019 o video napravah**).

se nanaša zahtevek, ali v pravno in tehnično analizo posameznih primerov na podlagi predvidene posebne obdelave in okoliščin upravljavca.

5) To mnenje ne obravnava obdelave osebnih podatkov otrok in ne posega v nobene posebne zahteve, ki veljajo v zvezi s tem.

6) To mnenje ne posega v pravne zahteve in nadaljnje omejitve glede uporabe biometričnih podatkov, ki izhajajo iz nacionalne zakonodaje držav članic[9].

7) Nobena ugotovitev v tem mnenju ne posega v nadaljnji tehnološki razvoj.

8) V tem mnenju so obravnavani štirje scenariji, njihove posebne značilnosti pa so opisane v nadaljevanju v oddelku 3.2. V njem se ne obravnavajo drugi scenariji, tudi če se obdelava izvaja za isti namen.

14. Francoski nadzorni organ je v zahtevku navedel, da bi obdelava biometričnih podatkov potnikov za pospešitev njihovega pretoka na letališčih temeljila na predpostavki, da posamezniki s tako obdelavo soglašajo, kar bi lahko bila pravna podlaga v skladu s Splošno uredbo o varstvu podatkov[10]. **Vendar analiza veljavne pravne podlage ne spada na področje uporabe vprašanj, predloženih EOVP v zahtevku, in tako v tem mnenju ni preučena veljavnost privolitve za tako obdelavo v skladu s 6., 7. in 9. členom Splošne uredbe o varstvu podatkov.**

15. Kljub temu EOVP na splošno ugotavlja, da bi morali zadevni upravljavci, če bi se zanašali na to pravno podlago, pridobiti veljavno izrecno privolitev[11] posameznikov, ki so take storitve pripravljeni uporabljati. Taka izrecna privolitev bi morala biti dana prostovoljno, konkretno in informirano[12], ali so ti pogoji izpolnjeni, pa bi se analiziralo za vsak primer posebej. To med drugim pomeni naslednje:

1) posamezniki bi morali imeti možnost, da tako privolitev kadar koli in brez kakršne koli škode preprosto prekličejo[13].

2) Da bi bila privolitev prostovoljna, se lahko biometrične tehnologije uporabljajo le prostovoljno, saj bi morali imeti posamezniki možnost, da se svobodno odločijo, ali bodo te storitve uporabljali ali ne, in sicer brez kakršne koli škode (kot je precej daljše

[9] Četrti odstavek 9. člena Splošne uredbe o varstvu podatkov na primer določa, da lahko države članice ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave biometričnih podatkov.
[10] Zahtevek, Priloga I.
[11] V skladu s štirinajstim odstavkom 4. člena in prvim odstavkom 9. člena ter točko a drugega odstavka 9. člena Splošne uredbe o varstvu podatkov je obdelava biometričnih podatkov za namene edinstvene identifikacije posameznika prepovedana, razen če je posameznik, na katerega se nanašajo osebni podatki, dal izrecno privolitev v obdelavo navedenih osebnih podatkov za enega ali več določenih namenov, razen kadar pravo Unije ali pravo države članice določa, da posameznik, na katerega se nanašajo osebni podatki, ne sme odstopiti od prepovedi iz prvega odstavka 9. člena Splošne uredbe o varstvu podatkov. Glej tudi uvodne izjave 51, 52 in 53 Splošne uredbe o varstvu podatkov.
[12] Enajsti odstavek 4. člena in 7. člen Splošne uredbe o varstvu podatkov.
[13] Četrti odstavek 7. člena in tudi uvodna izjava 50 Splošne uredbe o varstvu podatkov.

čakanje za potnike, ki ne privolijo[14]), spodbud, dodatnih stroškov ali dodatnih prednosti v zameno[15].

3) Za izrecno privolitev bi bilo treba zaprositi tudi posameznike, katerih biometrični podatki se obdelujejo, tudi če se niso prijavili za identifikacijo ali avtentikacijo s takimi sredstvi. Z drugimi besedami, bistveno je, da posameznikom, ki niso izrecno privolili v prepoznavanje obraza za predvideni namen, kamere ne bi optično brale obrazov. To se lahko na primer doseže tako, da se za prepoznavanje obrazov namenijo posebni pasovi ter zagotovijo ustrezne oznake in fizična ločitev od nebiometričnih kontrolnih tokov, da je mogoče take pasove jasno prepoznati.

4) Brez poseganja v to, ali bi bila privolitev veljavna pravna podlaga za tako obdelavo, se še vedno uporabljajo načela obdelave iz 5. člena Splošne uredbe o varstvu podatkov glede potrebnosti in sorazmernosti, tudi če so posamezniki izrecno privolili v uporabo biometričnih podatkov[16].

16. Zahtevek določa[17], da bodo upravljavci letališč delovali kot upravljavci v zvezi z obdelavo na varnostnih kontrolnih točkah na letališču, letalske družbe pa kot upravljavci v zvezi z obdelavo pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice. EOVP zato ugotavlja, da so lahko v obdelavo, opisano v zahtevku, vključeni različni akterji, in ni presojal uporabe vlog (skupnega) upravljavca in/ali obdelovalca v scenarijih, opisanih v nadaljevanju v oddelku 3.2 tega mnenja. Udeležene akterje je treba vsekakor opredeliti in jim jasno dodeliti odgovornosti, da bi bile izpolnjene zahteve iz Splošne uredbe o varstvu podatkov[18].

17. Poleg tega EOVP ugotavlja, da v EU za zdaj ni enotne pravne zahteve, po kateri bi morali upravljavci letališč in letalske družbe identificirati potnike ter na vseh navedenih kontrolnih točkah preveriti, ali se ime na vstopnem kuponu potnika ujema z imenom na njegovem osebnem dokumentu[19]. Zato za vse take zahteve velja nacionalna zakonodaja, ki se lahko med državami članicami razlikuje. V nekaterih državah članicah se lahko tako preverjanje zahteva na nekaterih kontrolnih točkah (na

[14] To bi lahko na primer vključevalo vidike, kot je oblikovanje sistema, s katerim bi se izognili ustvarjanju družbenega pritiska na potnike, ki ne želijo privoliti, in preprečili, da bi njihova izbira negativno vplivala na druge potnike.
[15] Smernice EOVP št. 05/2020 o privolitvi na podlagi Uredbe 2016/679, različica 1.1, sprejete 4. maja 2020 (v nadaljevanju: **Smernice EOVP 5/2020 o privolitvi**), točki 46 in 48.
[16] Prav tam, točka 5.
[17] Zahtevek, Priloga I.
[18] V skladu s sedmim in osmim odstavkom 4. člena in drugim odstavkom 5. člena ter 24., 26., 28. in 29. členom Splošne uredbe o varstvu podatkov. Glej tudi Smernice EOVP 07/2020 o pojmih upravljavec in obdelovalec iz Splošne uredbe o varstvu podatkov, različica 2.1, sprejete 7. julija 2021.
[19] Ustrezna uredba na ravni EU je Izvedbena uredba Komisije (EU) 2015/1998 z dne 5. novembra 2015 o določitvi podrobnih ukrepov za izvajanje skupnih osnovnih standardov za varovanje letalstva. Vendar ta uredba ne obravnava pregledov uradnih osebnih dokumentov na kontrolnih točkah na letališčih, države članice pa imajo diskrecijsko pravico, da to uredijo na nacionalni ravni.

primer pri oddaji prtljage ali vkrcanju), v drugih pa se taki pregledi za zdaj ne zahtevajo[20]. Obstoj pravnih obveznosti za preverjanje identitete potnikov neposredno vpliva na prakse različnih letališč.

18. Zato se v teh primerih, **kadar identitete potnikov ni treba preveriti z uradnim osebnim dokumentom, preverjanja ne bi smela izvajati z uporabo biometrije, saj bi se zaradi tega podatki pretirano obdelovali, ker bi se v primerjavi s sedanjim stanjem obdelali dodatni podatki in bi to presegalo tisto, kar je potrebno za zadevni namen, s čimer bi se kršilo načelo najmanjšega obsega podatkov iz točke c prvega odstavka 5. člena Splošne uredbe o varstvu podatkov.** Ta premislek je treba upoštevati pri preučitvi vseh scenarijev, opisanih v nadaljevanju v točki 3.2 tega mnenja.

2.2 Ključni pojmi

19. Da se podatki lahko štejejo za biometrične podatke v skladu s štirinajstim odstavkom 4. člena Splošne uredbe o varstvu podatkov[21], mora obdelava neobdelanih podatkov, kot so fizične, fiziološke ali vedenjske značilnosti fizične osebe, vključevati meritev teh značilnosti, ker so biometrični podatki rezultat takih meritev[22].

20. S posnetkom obraza posameznika (fotografijo ali videoposnetkom), kar se imenuje biometrični **vzorec**, je mogoče pridobiti digitalni prikaz različnih značilnosti zadevnega obraza (to se imenuje **predloga**)[23]. Poleg tega EOVP opozarja, da je „[b]iometrična predloga digitalni prikaz edinstvenih značilnosti, ki so bile pridobljene iz biometričnega vzorca in jih je mogoče shraniti v biometrično podatkovno zbirko[24],“ kar omogoča ali potrjuje edinstveno identifikacijo fizične osebe. Poleg tega naj bi bila „[t]a predloga edinstvena in specifična za vsakega posameznika, z vidika časa pa je načeloma trajna“[25]. Običajno se pri primerjavi, katere cilj je identifikacija ali avtentikacija posameznika s prepoznavanjem obraza, dohodna biometrična predloga primerja s shranjenimi predmeti, da se preveri ugotavljanje ujemanja ali poišče ujemanje v podatkovni zbirki[26].

[20] To pomeni, da se za zdaj preverjanje sploh ne izvaja ali pa se preverja samo obstoj vstopnega kupona. Državljani Norveške, Danske, Finske in Švedske so na primer od 1. julija 1954 na podlagi Protokola o izvzetju državljanov Danske, Finske, Norveške in Švedske iz obveznosti posedovanja potnega lista ali dovoljenja za prebivanje med prebivanjem v skandinavski državi, ki ni njihova matična država, z dne 22. maja 1954 izvzeti iz obveznosti posedovanja potnega lista ali druge potovalne identifikacije, kadar potujejo med temi državami.

[21] Glej tudi uvodne izjave 51, 52 in 53 Splošne uredbe o varstvu podatkov.

[22] Smernice EOVP 3/2019 o video napravah, točka 74.

[23] Smernice EOVP 05/2022 o uporabi tehnologij za prepoznavanje obraza na področju preprečevanja, odkrivanja, preiskovanja ali pregona kaznivih dejanj, različica 2.0, sprejete 26. aprila 2023 (v nadaljevanju: **Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj**), točki 7 in 8.

[24] Prav tam, točka 9.

[25] Prav tam.

[26] Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točki 10 in 11; glej tudi mednarodni standard ISO/IEC 2382-37, 2022-03, na voljo na: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [nazadnje obiskano 23. maja 2024] (v nadaljevanju: **standard ISO/IEC 2382-37**).

21. Tehnologija za prepoznavanja obrazov lahko opravlja dve ločeni funkciji – avtentikacijo[27] in identifikacijo[28]. Čeprav se funkciji razlikujeta, temeljita na obdelavi biometričnih podatkov, povezanih z določeno ali določljivo fizično osebo[29], in zato pomenita obdelavo posebnih vrst osebnih podatkov v skladu z 9. členom Splošne uredbe o varstvu podatkov[30].

22. Zlasti:

> **Avtentikacija** je namenjena potrjevanju biometričnih podatkov s primerjavo. To se imenuje tudi preverjanje „ena proti ena“.
>
> **Identifikacija** je namenjena iskanju po podatkovni zbirki biometričnih vpisov, da se vrnejo identifikatorji, ki jih je mogoče pripisati enemu samemu posamezniku. Imenuje se tudi identifikacija „ena proti mnogo“.

23. V obeh primerih tehnike za prepoznavanje obraza (tj. identifikacija in avtentikacija) temeljijo na oceni ujemanja med predlogami, in sicer med primerjanimi predlogami in izhodiščem(-i). S tega vidika delujejo na podlagi verjetnosti: s primerjavo se določi večja ali manjša verjetnost, da je oseba resnično oseba, ki jo je treba avtentificirati ali identificirati; če ta verjetnost preseže določen prag v sistemu, ki ga določi uporabnik ali razvijalec sistema, bo sistem domneval, da obstaja ujemanje, ki ga je treba identificirati ali avtenticirati[31].

[27] EOVP ugotavlja, da je v prihodnji uredbi Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci) (še ni objavljen v Uradnem listu) „biometrično preverjanje“ v šestintridesetem odstavku 3. člena opredeljeno tudi kot „avtomatizirano preverjanje ‚ena proti ena‘, vključno z avtentikacijo, identitete fizičnih oseb s primerjavo njihovih biometričnih podatkov s predhodno pridobljenimi biometričnimi podatki“ (glej Zakonodajno resolucijo Evropskega parlamenta z dne 13. marca 2024 o predlogu uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov Unije (COM(2021) 0206) – C9-0146/2021 – 2021/0106(COD)).

[28] Enako je v petintridesetem odstavku 3. člena Akta o umetni inteligenci „biometrična identifikacija“ opredeljena kot „avtomatizirano prepoznavanje fizičnih, fizioloških, vedenjskih ali psiholoških lastnosti človeka z namenom ugotavljanja identitete fizične osebe s primerjavo biometričnih podatkov tega posameznika z biometričnimi podatki posameznikov, shranjenimi v podatkovni zbirki“.

[29] Standard ISO/IEC 2382-37.

[30] Štirinajsti odstavek 4. člena Splošne uredbe o varstvu podatkov in Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točka 12.

[31] Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točka 11. Glej tudi standard ISO/IEC 2382-37.

3 O UTEMELJENOSTI ZAHTEVKA

3.1 Splošne opombe

24. V tem razdelku so analizirana vprašanja, predstavljena zgoraj v točki 4. EOVP bo v zvezi s tem za prvo vprašanje analiziral združljivost s točko f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov, za drugo vprašanje pa združljivost s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov.

25. Zato bo EOVP analiziral štiri različne scenarije[32], katerih posebne značilnosti so opisane v nadaljevanju v oddelku 3.2.

26. EOVP uvodoma opozarja, da uporaba biometričnih podatkov in zlasti tehnologije za prepoznavanje obrazov pomeni večja tveganja za pravice in svoboščine posameznikov. Prvič, zadevna obdelava se nanaša na biometrične podatke, ki se jim v skladu z 9. členom Splošne uredbe o varstvu podatkov zagotavlja posebno varstvo. Biometrični podatki nepovratno spreminjajo odnos med telesom in identiteto, ker omogočajo, da so značilnosti človeškega telesa „strojno berljive“ in se nadalje uporabljajo[33]. Poleg tega lahko uporaba tehnologije za prepoznavanje obrazov povzroči tveganja, povezana z lažno negativnimi rezultati, pristranskostjo in diskriminacijo[34], možnost zlorabe biometričnih podatkov pa bi lahko imela resne posledice za posameznike, kot sta identitetna prevara ali goljufija po podobnosti[35]. Opozoriti je treba tudi, da so posamezniki, kadar se prepoznavanje obrazov izvaja na daljavo in brez njihovega dejavnega sodelovanja, morda še manj seznanjeni s tako obdelavo in povezanimi tveganji. Nazadnje je treba poudariti, da se lahko značilnosti, na katerih temeljijo biometrični podatki, na splošno štejejo za trajne in bi jih bilo treba obravnavati kot nepreklicne, zlasti v okviru prepoznavanja obrazov[36].

27. Zato bi morali upravljavci ob upoštevanju navedenega pred uporabo takih tehnologij, tudi če bi se štele za posebej učinkovite, oceniti, kakšen je njihov učinek na temeljne pravice in svoboščine

---

[32] Štirje scenariji, ki jih je analiziral EOVP, temeljijo na primerih uporabe, predstavljenih v Prilogi I k zahtevku. Francoski nadzorni organ je pojasnil, da so primeri uporabe, predstavljeni v Prilogi I k zahtevku, primeri izvajanja, ki spadajo v scenarij in se uporabljajo za ponazoritev.

[33] Mnenje delovne skupine iz člena 29 št. 3/2012 o razvoju na področju biometričnih tehnologij, sprejeto 27. aprila 2012, WP 193 (v nadaljevanju: **Mnenje delovne skupine iz člena 29 št. 3/2012 o biometričnih tehnologijah**), str. 4. Opozoriti je treba, da se to mnenje nanaša na Direktivo 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Direktiva o varstvu podatkov). S Splošno uredbo o varstvu podatkov se je razširilo področje uporabe posebnih vrst podatkov, drugače kot v Direktivi o varstvu podatkov pa je v njej določeno, da so biometrični podatki posebne vrste podatkov (9. člen Splošne uredbe o varstvu podatkov).

[34] *Guidelines on facial recognition* (Smernice o prepoznavanju obrazov), Posvetovalni odbor iz Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, junij 2021, str. 15; tudi Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točka 27.

[35] Mnenje delovne skupine iz člena 29 št. 3/2012 o biometričnih tehnologijah, str. 29.

[36] Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točka 104.

posameznikov ter preučiti, ali se lahko njihov zakoniti namen obdelave doseže s sredstvi, ki manj posegajo v zasebnost[37].

28. EOVP tudi opozarja, da pravica do varstva osebnih podatkov ni absolutna pravica in bi jo bilo treba v skladu z načelom sorazmernosti uravnotežiti z drugimi temeljnimi pravicami, zaščitenimi z Listino[38].

29. Prvi odstavek 25. člena Splošne uredbe o varstvu podatkov se nanaša na „načela varstva podatkov“, navedena v 5. členu Splošne uredbe o varstvu podatkov[39], ter zahteva, da se njihovo varstvo vgrajeno izvaja „učinkovito“[40]. To izrecno vključuje načelo najmanjšega obsega podatkov iz točke c prvega odstavka 5. člena Splošne uredbe o varstvu podatkov[41], v skladu s katerim morajo biti osebni podatki „ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo, s čimer se izraža načelo sorazmernosti“[42]. Poleg tega je v drugem odstavku 25. člena Splošne uredbe o varstvu podatkov določena obveznost „privzete obdelave najmanjšega obsega podatkov“ z navedbo, da velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost[43].

30. Vendar 25. člen Splošne uredbe o varstvu podatkov od upravljavcev ne zahteva, da izvedejo posebne tehnične in organizacijske ukrepe, ampak da morajo biti izbrani ukrepi in zaščitni ukrepi specifični glede na okoliščine in tveganja za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki jih pomeni obdelava[44]. Podobno 32. člen Splošne uredbe o varstvu podatkov o varnosti obdelave od upravljavcev in obdelovalcev zahteva, da izvedejo ustrezne tehnične in organizacijske

---

[37] Uvodna izjava 39 Splošne uredbe o varstvu podatkov. Glej tudi Smernice EOVP 3/2019 o video napravah, točka 73.

[38] Uvodna izjava 4 Splošne uredbe o varstvu podatkov. Glede tega glej tudi sodbo Sodišča z dne 22. junija 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (v nadaljevanju: sodba v zadevi C-439/19, *Latvijas Republikas Saeima*), točke 98, 110 in 113. Poleg tega se na podlagi načela sorazmernosti kot splošnega načela prava EU zahteva, da so ukrepi, sprejeti na podlagi akta Unije, primerni za uresničitev cilja, na katerega se akt nanaša, in da ne prekoračijo okvirov, ki so potrebni za njegovo doseganje (glej sodbo Sodišča z dne 9. novembra 2010, *Volker und Markus Schecke in podjetje Eifert*, C-92/09 in C-93/09, ECLI:EU:C:2010:662 (v nadaljevanju: sodba v združenih zadevah C-92/09 in C-93/09, *Volker und Schecke*), točka 74 in navedena sodna praksa).

[39] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, različica 2.0, sprejete 20. oktobra 2020 (v nadaljevanju: **Smernice EVOP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov**), točka 11.

[40] Prvi odstavek 25. člena Splošne uredbe o varstvu podatkov določa: „Ob upoštevanju najnovejšega tehnološkega razvoja, stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki so povezana z obdelavo in se razlikujejo po verjetnosti in resnosti, upravljavec tako v času določanja sredstev obdelave kot tudi v času same obdelave izvaja ustrezne tehnične in organizacijske ukrepe, kot je psevdonimizacija, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, kot je načelo najmanjšega obsega podatkov, ter v obdelavo vključi potrebne zaščitne ukrepe, da se izpolnijo zahteve te uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.“ Glej tudi Smernice EVOP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 13.

[41] V uvodni izjavi 39 Splošne uredbe o varstvu podatkov je navedeno, da bi se lahko osebni podatki obdelali le, če namena obdelave ne ni bilo mogoče razumno doseči z drugimi sredstvi.

[42] Sodba v zadevi C-439/19, *Latvijas Republikas Saeima*, točka 98; sodba Sodišča z dne 11. decembra 2019, *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (v nadaljevanju: sodba v zadevi C-708/18, *M5A-ScaraA*), točka 48.

[43] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 48.

[44] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 14.

ukrepe za zagotovitev ustrezne ravni varnosti glede na tveganje za pravice in svoboščine posameznikov.

31. Tudi če bi potniki izrecno privolili v uporabo biometričnih podatkov, da bi se pospešil njihov pretok na letališčih, je pomembno, da se načela obdelave iz Splošne uredbe o varstvu podatkov glede potrebnosti in sorazmernosti še vedno uporabljajo in jih je treba upoštevati[45].

32. EOVP bo glede **načela potrebnosti** preučil, ali je predlagana obdelava potrebna za doseganje postavljenega cilja in ali je mogoče isti cilj enako učinkovito doseči z drugimi sredstvi, ki manj posegajo v temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki[46]. Glede **načela sorazmernosti** bo ocenil, ali je negativni vpliv na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, sorazmeren s pričakovano koristjo. Če je korist razmeroma majhna, tak vpliv morda ni sorazmeren[47].

33. Tudi če EOVP meni, da bi lahko eden od scenarijev, analiziranih v nadaljevanju, izpolnjeval zahteve iz točk e in f prvega odstavka 5. člena ter 25. in 32. člena Splošne uredbe o varstvu podatkov, mora upravljavec v vsakem primeru to dokazati z dejanskimi elementi. Pri taki predstavitvi bi bilo treba preučiti alternativne scenarije.

3.2 O združljivosti s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov

3.2.1 Scenarij 1: hramba vpisane biometrične predloge za avtentikacijo le pri posamezniku

34. V tem oddelku je preučeno, ali je hramba biometrične predloge potnikov le pri posamezniku, na primer na njegovi osebni napravi[48], ki je pod njegovim izključnim nadzorom[49], za avtentikacijo[50] združljiva s točko f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov (v nadaljevanju: **scenarij 1**). V tem oddelku so preučeni tudi ustrezni zaščitni ukrepi za scenarij 1 glede na 25. in 32. člen Splošne uredbe o varstvu podatkov.

Opis scenarija

35. V scenariju 1 vpisano biometrično predlogo vsakega potnika, ki je privolil v tako obdelavo, hrani le posameznik, na primer na osebni napravi, ki je pod izključnim nadzorom vsakega potnika. Potniki se avtenticirajo (primerjava „ena proti ena“), ko gredo skozi posamezne kontrolne točke na letališču.

[45] Smernice EOVP št. 05/2020 o privolitvi na podlagi Uredbe 2016/679, točka 5.
[46] Sodba v zadevi C-439/19, *Latvijas Republikas Saeima*, točki 110 in 113 ter sodba Sodišča (veliki senat) z dne 4. julija 2023, *Meta proti Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, točka 108.
[47] Sodba v zadevi C-708/18, *M5A-ScaraA*, točke 52 do 56, sodba v združenih zadevah C-92/09 in C-93/09, *Volker und Schecke*, točka 87, ter sodba v zadevi C-439/19, *Latvijas Republikas Saeima*, točke 98, 110 in 113. Glej tudi Mnenje delovne skupine iz člena 29 št. 3/2012 o biometričnih tehnologijah, str. 8.
[48] Druga možnost je, da posameznik biometrično predlogo natisne na papir in jo hrani.
[49] To ne posega v splošno odgovornost upravljavca glede obdelave.
[50] Kot je ponazorjeno s primerom uporabe 1 v Prilogi I k zahtevku.

36. Vpis opravi upravljavec letališča, in sicer na daljavo prek svoje aplikacije[51], ali na letaliških terminalih z ustrezno ravnjo zanesljivosti identitete (na primer raven zanesljivosti, ki ustreza ravni po uredbi eIDAS[52]). Tak vpis zajema beleženje biometrične predloge in identifikacijskih podatkov na napravi potnika[53], ki so potrebni za obdelavo. Vpis se izvede le enkrat in za določeno obdobje veljavnosti (ki je na primer usklajeno z obdobjem veljavnosti potnega lista potnika). Upravljavec letališča po vpisu ne hrani niti identifikacijskih niti biometričnih podatkov potnikov.

37. Zlasti kar zadeva hrambo, se identifikacijski podatki potnika in biometrična predloga hranijo lokalno na napravi vsakega potnika (na primer v mobilni aplikaciji upravljavca letališča ali aplikaciji digitalne denarnice). Naprava se nato lahko uporabi za prenos ali poizvedovanje po identifikacijskih podatkih in biometrični predlogi potnika, kar po možnosti zajema tudi informacije o letu in/ali vstopnem kuponu. Te informacije so na primer šifrirane s ključem, ki ga ima le upravljavec letališča – morda kodirane v obliki kode QR, ki se lahko natisne na papir ali prikaže na zaslonu naprave potnika. V tem primeru bi potnik to kodo QR nato pokazal v namenskih kontrolnih terminalih na letališču, opremljenih z optičnim bralnikom kod QR in kamero.

38. Kar zadeva varnost, se kode QR med ugotavljanjem ujemanja dešifrirajo s ključem, ki ga ima upravljavec letališča, saj je edini, ki jih lahko dešifrira. Biometrični podatki potnikov se hranijo le zelo kratek čas in se izbrišejo po tem, ko je ugotavljanje ujemanja končano. Opozoriti je treba, da so varnostni ukrepi glede hrambe delno odvisni od varnosti potnikove naprave.

Ocena EOVP

39. V scenariju 1 so opisani tehnični in organizacijski ukrepi, zasnovani tako, da zagotavljajo raven varnosti, ki ustreza tveganjem za posameznike, na katere se nanašajo osebni podatki, kot se zahteva v skladu s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov. Potniki se avtenticirajo (primerjava „ena proti ena“), ko gredo skozi posamezne kontrolne točke na letališču. V tem scenariju se glavni postopek ugotavljanja ujemanja izvede v nadzorovanem okolju[54], kjer potniki dejavno sodelujejo in imajo več nadzora nad svojimi podatki. Preverjali bi se namreč le potniki, ki so v tako obdelavo privolili. Ker bi to preverjanje potekalo na namenskih terminalih, pa se ne bi zbirali biometrični podatki drugih potnikov, ki v tako obdelavo niso privolili. Poleg tega lahko potniki, ki dajo privolitev, kadar koli ustavijo obdelavo, tako da izbrišejo podatke iz svoje naprave.

40. Uporaba prepoznavanja obrazov na podlagi biometrične predloge, ki jo hrani le posameznik, na primer na osebni napravi, ki je pod izključnim nadzorom potnika in se uporablja za avtentikacijo na

[51] EOVP ugotavlja, da bi se lahko v prihodnosti določili drugi načini za tak vpis, ki bi se morda lahko izvedel brez posebne aplikacije upravljavca letališča, tako da se na primer omogoči interakcija z digitalno denarnico uporabnika.

[52] Okvir za elektronsko identifikacijo in storitve zaupanja (electronic identification and trust services – **eIDAS**) na podlagi Uredbe (EU) 2024/1183 Evropskega parlamenta in Sveta z dne 11. aprila 2024 o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za digitalno identiteto.

[53] V tem mnenju identifikacijski podatki pomenijo podatke, kot so priimek, ime, datum rojstva itd., ki so bili preverjeni kot točni glede na osebni dokument ali potni list.

[54] „Nenadzorovano okolje“ se nanaša na uporabo prepoznavanja obrazov za identifikacijo brez dejavnega sodelovanja posameznikov, na katere se nanašajo osebni podatki, kadar se predloga obraza vsake osebe, ki vstopa na območje spremljanja, primerja s predlogami širokega preseka prebivalstva, shranjenimi v podatkovni zbirki; glej Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točka 17.

posameznih kontrolnih točkah prek namenskega vmesnika, pod določenimi pogoji pomeni manjše tveganje kot uporaba biometričnih podatkov, ki se hranijo v centralizirani podatkovni zbirki[55]. S tako lokalizirano hrambo se, če jo spremljajo ustrezni zaščitni ukrepi[56], zmanjšuje resnost kršitev varstva osebnih podatkov v primerjavi s centralizirano hrambo glede na število prizadetih posameznikov in zagotavlja, da posameznik, na katerega se nanašajo osebni podatki, dejavno sodeluje pri dostopu do biometrične predloge.

41. Poleg tega bi se lahko ugotavljanje ujemanja izvedlo lokalno na letališču, in sicer s primerjavo biometrične predloge, ki jo na primer vsebuje koda QR, in izpisa predloge, izračunanega na podlagi biometričnega vzorca, zajetega s kamero kontrolnega terminala. Kontrolor, ki opravlja poseben pregled (ki je lahko upravljavec letališča ali letalska družba, odvisno od tega, ali se opravi na varnostnih kontrolnih točkah na letališču, pri oddaji prtljage, vkrcanju in/ali dostopu do potniške čakalnice), pa pozna in uporablja le rezultat ugotavljanja ujemanja. Poleg tega dejstvo, da mora posameznik navesti informacije, potrebne za ugotavljanje ujemanja (na primer kodo QR), deluje kot drugi dejavnik[57] in tako krepi varnost avtentikacije.

42. Glede združljivosti s 25. členom Splošne uredbe o varstvu podatkov in zlasti za izpolnitev zahteve glede najmanjšega obsega podatkov je treba zagotoviti, da obdelava izpolnjuje načelo potrebnosti. V scenariju 1 bi se lahko štelo, da izbrani ukrepi izpolnjujejo načelo potrebnosti v zvezi z namenom, ki se želi doseči (tj. pospešitev pretoka potnikov), če lahko upravljavec glede na okoliščine obdelave dokaže, da ni alternativnih rešitev, ki manj posegajo v zasebnost, s katerimi bi se lahko enako učinkovito dosegel isti cilj. Upravljavec lahko na primer dokaže, da bi se s scenarijem 1, tudi če bi morali potniki pokazati svojo napravo, pospešil postopek preverjanja v primerjavi s sedanjim stanjem, pri katerem preverjanje, ki ga opravijo ljudje, zajema ugotavljanje, ali se ime na vstopnem kuponu ujema z osebnim dokumentom potnika[58]. Tega zlasti ne bi bilo mogoče dokazati, če se trenutno ne preverja identiteta potnikov na podlagi njihovega uradnega osebnega dokumenta (glede tega glej točko 18 zgoraj).

43. Poleg tega upravljavec letališča biometričnih predlog po vpisu ne hrani, upravljavec, ki preverjanje opravi, pa biometrične podatke hrani zelo kratek čas, saj se taki podatki izbrišejo takoj, ko je ugotavljanje ujemanja končano. Zato se zdi, da ukrepi, izbrani v scenariju 1, omejujejo obseg obdelave in obdobje hrambe osebnih podatkov.

44. Kar zadeva načelo sorazmernosti, se lahko poseganje v zasebnost pri taki obdelavi uravnoteži z dejavnim sodelovanjem potnikov, saj bi svoje biometrične podatke hranili le oni sami. Poleg tega bi lahko ob upoštevanju opisanih ukrepov in ob predpostavki, da upravljavec izvaja ustrezne zaščitne ukrepe, kot se zahtevajo z zadevno posebno obdelavo, izvajanje ustreznih ukrepov zagotovilo raven varnosti, ki ustreza tveganju. V tem primeru bi se lahko negativni vpliv na temeljne pravice in svoboščine posameznikov štel za sorazmernega s pričakovano koristjo.

[55] Smernice EOVP 05/2022 o prepoznavanju obraza pri preprečevanju, odkrivanju, preiskovanju ali pregonu kaznivih dejanj, točka 17.
[56] Kot je navedeno v nadaljevanju v točki 46.
[57] S tem se na primer zmanjša tveganje za slepljenje identitete. Glej tudi varnostni ukrep C.1.2 v nadaljevanju.
[58] Lahko bi tudi trdili, da so napake pri biometričnem preverjanju manj verjetne kot pri preverjanju, ki ga opravijo ljudje.

45. Zato EOVP ob upoštevanju navedenega v odgovoru na vprašanje 1.1 ugotavlja, da bi se **lahko načeloma štelo,** da je taka obdelava **združljiva s točko f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov, če bi se izvajali ustrezni zaščitni ukrepi**.

Ustrezni zaščitni ukrepi

46. EOVP v takem scenariju v odgovoru na vprašanje 1.2 meni, da bi bilo treba izvajati vsaj naslednje zaščitne ukrepe. *Za doseganje istih ciljev glede varnosti in varstva podatkov bi se lahko poleg zaščitnih ukrepov, opisanih v tem mnenju, uporabili tudi drugi zaščitni ukrepi, ki bi lahko bili zakoniti, če bi zagotavljali skladnost z veljavnim pravnim okvirom*.

47. Opomba: *to je neizčrpen pregled morebitnih ustreznih zaščitnih ukrepov na visoki ravni, ki bi jih moral upravljavec izvajati pri rešitvi, podobni scenariju 1. Njihova ustreznost v skladu s 25. in 32. členom Splošne uredbe o varstvu podatkov bo odvisna od analize posameznih primerov. Vsi upravljavci bodo morali zagotoviti, da bodo izvedli lastno oceno učinka v zvezi z varstvom podatkov[59], zaradi njihovih posebnih rešitev pa bi lahko bili potrebni dodatni ukrepi, ki v to mnenje niso vključeni*.

A. Splošni

A.1 Ocena učinka v zvezi z obdelavo podatkov

A.1.1 Vsakič, ko upravljavec načrtuje nov postopek obdelave, v katerega je zajeta obdelava, ki bi lahko povzročila veliko tveganje, izvesti oceno učinka v zvezi z varstvom podatkov v skladu z zahtevami iz 35. člena Splošne uredbe o varstvu podatkov. To bo verjetno veljalo za scenarij 1, saj vključuje obsežno obdelavo biometričnih podatkov[60]. Oceniti, ali se sistem za prepoznavanje obrazov, vključno z njegovo potrebnostjo in sorazmernostjo glede na predvideni namen[61], v zgodnji fazi zasnove ustrezno izvaja, in ga pregledovati v celotnem življenjskem ciklu razvoja izdelka.

A.1.2 Posvetovati se z ustreznim nadzornim organom, če bi obdelava kljub ukrepom, ki jih je upravljavec sprejel za zmanjšanje tveganja, še vedno povzročila veliko tveganje[62].

A.2 Pravice posameznikov, na katere se nanašajo osebni podatki, in zaščitni ukrepi, ki jih lahko izvajajo upravljavci

A.2.1 Zaščitni ukrepi za obravnavanje primerov lažno negativnih rezultatov. Zmanjšati tveganje starostne, spolne in rasne pristranskosti, tako da se „redno ocenjuje, ali algoritmi delujejo v skladu z nameni, in se prilagaja algoritme tako, da blažijo odkrite pristranskosti ter

[59] Člen 35 Splošne uredbe o varstvu podatkov.
[60] Tretji odstavek 35. člena Splošne uredbe o varstvu podatkov in Smernice delovne skupine iz člena 29 glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, sprejete 13. oktobra 2017, Wp248rev.01, ki jih je podprl EOVP.
[61] Točka b sedmega odstavka 35. člena Splošne uredbe o varstvu podatkov.
[62] Prvi odstavek 36. člena Splošne uredbe o varstvu podatkov.

zagotavljajo pravičnost pri obdelavi“[63]. Na primer s človeškim nadzorom in posredovanjem, da bi se ublažila morebitna pristranskost in preprečila stigmatizacija ali profiliranje potnikov.

A.2.2 Zagotoviti, da je vsaka obdelava osebnih podatkov pregledna ter da so posamezniki seznanjeni s tem in imajo pri vsakem postopku obdelave nadzor nad tem, kako se obdelujejo njihovi podatki[64].

A.2.3 Zagotoviti, da so vzpostavljeni ukrepi za zagotavljanje skladnosti z načelom omejitve namena, tako da se podatki ne uporabljajo za druge namene, kot sta varnost ali usposabljanje.

A.2.4 Z ustreznimi ukrepi zagotoviti, da ni zajeta nobena fotografija ali videoposnetek posameznikov, ki v prepoznavanje obrazov ne privolijo, tudi če nista posneta in obdelana (kot je uporaba ustrezne globinske ostrine in območja za zajem, da se prepreči zajemanje slik drugih potnikov v ozadju ali okolici, uvedba namenskih čakalnih vrst, jasno označenih za prepoznavanje obrazov).

A.2.5 Če lahko iste terminale uporabljajo potniki, ki v prepoznavanje obrazov privolijo, in tisti, ki v to ne privolijo, ali kadar se lahko potniki, ki v prepoznavanje obrazov ne privolijo, med tem ko se sistem ne uporablja, pojavijo v vidnem polju, pred začetkom zajema fotografije ali videoposnetka počakati na pozitivno dejanje potnika, ki je v zajem privolil.

A.2.6 Omogočiti posamezniku, da lahko kadar koli izbriše podatke, ki so izključno v njegovi lasti (biometrična predloga)[65], kot se hranijo v mobilni aplikaciji ali digitalni denarnici[66].

A.2.7 Zagotoviti obstoj izvedljivih alternativ ali nadomestnih rešitev (tj. za potnike, ki ne bi privolili v uporabo biometričnih podatkov, potnike, ki takih rešitev ne bi mogli uporabljati, ali potnike, ki so bili napačno zavrnjeni), da se zagotovi tudi, da potniki, ki v uporabo ne privolijo, ne utrpijo nobene škode[67].

A.2.8 Če se uporablja aplikacija, jo je treba skrbno načrtovati in konfigurirati, da se ne zbirajo nepotrebni podatki in da se prepreči uporaba kompletov za razvoj programske opreme tretjih oseb, ki zbirajo podatke za druge namene.

A.3 Odgovornost

A.3.1 Oceniti, ali obstajajo ustrezni kodeksi ravnanja ali mehanizmi potrjevanja, s katerimi bi se lahko dokazala skladnost z varnostjo obdelave iz 32. člena Splošne uredbe o varstvu

[63] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, opomba 60, točka 70.
[64] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 68, in uvodna izjava 7 Splošne uredbe o varstvu podatkov.
[65] Sklici na biometrično predlogo v zaščitnih ukrepih v scenariju 1 ustrezajo sklicem na ključ oziroma skrivni podatek v scenariju 2.
[66] Upoštevajte, da ta zaščitni ukrep velja samo za 1. scenarij.
[67] Smernice EOVP 3/2019 o video napravah, točka 86.

podatkov[68]. Preveriti ustreznost ukrepov za posamezno zadevno obdelavo. Pri določanju ustreznih ukrepov so lahko koristni standardi[69], dobra praksa ter kodeksi ravnanja, ki jih priznavajo združenja in drugi organi, ki zastopajo kategorije upravljavcev.

A.3.2 Zagotoviti, da se na napravi uporabnika izvajajo osnovni varnostni pregledi, da se omogoči faza vpisa, čeprav pri varstvu svojih podatkov sodeluje tudi potnik, saj jih hrani na svoji napravi. Primeri takih tehničnih pregledov in kontrol so predstavljeni v oddelku C.2 Infrastruktura in omrežje.

B. Organizacijski:

B.1 Politika in skladnost

B.1.1 Zagotoviti, da je vzpostavljen notranji nadzor dostopa[70] s pravili za administratorje.

B.1.2 Če lahko storitev prepoznavanja obrazov zagotovi ena od strani, ki sodeluje pri obdelavi, ne da bi morale druge udeležene strani obdelati identifikacijske ali biometrične podatke ali podatke obeh vrst, prepovedati pretok teh podatkov prek teh drugih strani. Letalski družbi na primer ni treba tehnično dostopati do biometričnih podatkov, kadar se zanaša na skupno letališko infrastrukturo, tudi če deluje kot upravljavec obdelave v skladu s Splošno uredbo o varstvu podatkov.

B.1.3 Opredeliti politiko za šifriranje in upravljanje ključev[71], na primer za obdelavo identifikacijskih in biometričnih podatkov.

B.1.4 Zagotoviti skladnost s 5. poglavjem Splošne uredbe o varstvu podatkov. Da se na primer zagotovijo skladni prenosi, če upravljavec med postopkom vpisa uporablja storitev na daljavo, ki ima sedež v tretji državi.

B.1.5 V primeru obdelave s strani obdelovalcev zagotoviti, da je z njimi sklenjena pogodba[72] v skladu s tretjim odstavkom 28. člena Splošne uredbe o varstvu podatkov.

B.1.6 Zagotoviti, da so vzpostavljeni postopki za upravljanje človeškega nadzora in posredovanja, zlasti za obravnavanje težav z napačnimi zavrnitvami ter tehničnih težav ali težav z uporabnostjo.

B.2 Usposabljanje in testiranje

[68] Tretji odstavek 32. člena Splošne uredbe o varstvu podatkov in Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 10.
[69] Glej na primer standard ISO/IEC 2382-37.
[70] Smernice EOVP št. 04/2020 o uporabi lokacijskih podatkov in orodij za sledenje stikom v okviru izbruha COVID-19, sprejete 21. aprila 2020 (v nadaljevanju: **Smernice EVOP št. 04/2020 o lokacijskih podatkih in orodjih za sledenje stikom**), SEC-10, str. 16.
[71] Smernice EOVP 3/2019 o video napravah, točka 89.
[72] Tretji odstavek 28. člena Splošne uredbe o varstvu podatkov.

B.2.1. Zagotoviti, da je osebje ustrezno usposobljeno.

B.2.2 Izvajati „postop[ek] rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave“[73].

B.2.3 Izvesti postopek za zagotovitev, da je obdelava biometrične predloge potnika[74] za avtentikacijo tehnično učinkovita in dovolj natančna.

B.2.4 Zagotoviti, da so biometrični vzorci, zbrani ob vpisu in na kontrolni točki, dovolj kakovostni za zanesljivo obdelavo biometričnih podatkov.

C. Tehnični:

C.1 Dostop

C.1.1 Izvajati zaščitne ukrepe v fazi vpisa, da se zagotovi samovzorčenje vpisa s preverjeno identiteto. Da bi se okrepilo ocenjevanje identitete uporabnikov z večfaktorsko avtentikacijo, se lahko na primer izvedejo koraki, ki segajo od enkratnih povezav, zaščitenih z geslom, za zagon aplikacije do mehanizmov za deblokiranje lokalnih naprav.

C.1.2 Izvajati zaščitne ukrepe za obravnavanje primerov lažno pozitivnih rezultatov, napadov s predstavitvijo in preprečevanje goljufij[75].

C.1.3 Prepovedati zunanji dostop do identifikacijskih in biometričnih podatkov[76].

C.1.4 Zagotoviti, da obdelava v fazah vpisa, prenosa in ugotavljanja ujemanja poteka lokalno. Točka ugotavljanja ujemanja mora biti čim bližje napravi posameznika. Da bi se omogočilo ugotavljanje ujemanja predlog v osebni napravi, bi morda morali sodelovati ponudniki storitev, ki so zunaj letališča, pri tem pa bi se uporabljali viri javnega omrežja, kar bi negativno vplivalo na razpoložljivost in omogočilo prenos predloge zunanjim subjektom.

C.1.5 Avtenticirati uporabnika, da se doda nov let in ustvari nova šifrirana koda QR.

C.1.6 Izvajati ukrepe za obravnavanje primerov, v katerih lahko potnik izgubi dostop do kode QR.

C.2 Infrastruktura in omrežje

[73] Točka d prvega odstavka 32. člena Splošne uredbe o varstvu podatkov.
[74] Sklici na biometrično predlogo v zaščitnih ukrepih v 1. scenariju ustrezajo sklicem na ključ oziroma skrivni podatek v 2. scenariju.
[75] Poročilo agencije ENISA o digitalni identiteti o spodbujanju pojma samoupravljana identiteta za utrditev zaupanja iz januarja 2022.
[76] Smernice EOVP 3/2019 o video napravah, točka 89.

C.2.1 Posodabljati pogoje za delovanje operacijskega sistema in omogočati avtentikacijo za dostop do naprave za delovanje aplikacije oziroma digitalne denarnice, vključno s samodejnim izbrisom identifikacijskih in biometričnih podatkov, če je operacijski sistem zastarel in pomeni varnostno tveganje.

C.2.2 Osamiti enote za ugotavljanje ujemanja (tj. terminale) iz omrežja med obratovanjem in sprejeti vse druge potrebne ukrepe za zagotovitev varnosti.

C.2.3 Opraviti ugotavljanje ujemanja biometričnih podatkov na napravi potnika ali na terminalu (računalništvo na robu);

C.2.4 Poiskati rešitve za odpravo varnostnih ranljivosti posameznih naprav potnikov, vključno s šifriranjem (vsaj) biometričnih in identifikacijskih podatkov v mirovanju.

C.2.5 Uporabiti varno hrambo (vsaj) biometričnih podatkov izključno pri uporabniku[77], na primer z uporabo varne enklave na pametnem telefonu.

C.2.6 Uvesti varnostne ukrepe, da se zagotovi fizična varnost prostorov, vključno z biometričnim terminalom na letališču. Zagotoviti visoko raven varnosti za elemente arhitekture, ki obdelujejo (na primer izračun, pretok podatkov, začasna ali dolgoročna hramba) identifikacijske in biometrične podatke.

C.3 Varnost in upravljanje podatkov za preverjanje identitete uporabnika

C.3.1 Podatke med prenosom in hrambo razdeliti v vsaj tri različne skupine, na primer na identifikacijske in biometrične podatke ter podatke o letu[78]. Zagotoviti, da so podatki med prenosom in hrambo ustrezno šifrirani.

C.3.2 Vzpostaviti tehnične ukrepe, da bi se na kontrolni točki obdelovali in preverjali le podatki, ki se lahko zakonito obdelujejo na posameznih kontrolnih točkah.

C.3.3 Zagotoviti učinkovitost izbrisa podatkov[79] z varnim postopkom izbrisa (na primer glavni pomnilnik, predpomnilnik, morebitne varnostne kopije) in oceniti, kdaj bi bilo treba podatke samodejno izbrisati. Obdobja hrambe podatkov bi bilo treba strogo upoštevati s samodejnimi rutinami, ne da bi moral posameznik dodatno ukrepati[80].

C.3.4 Zagotoviti verodostojnost in celovitost podatkov (na primer podpis)[81].

[77] Sklici na biometrično predlogo v zaščitnih ukrepih v 1. scenariju ustrezajo sklicem na ključ oziroma skrivni podatek v 2. scenariju.
[78] Smernice EOVP 3/2019 o video napravah, točka 89.
[79] Smernice EOVP 3/2019 o video napravah, točka 89.
[80] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 82.
[81] Smernice EOVP 3/2019 o video napravah, točka 89.

C.3.5 Hraniti biometrične podatke potnikov na točki vpisa in kontrolni točki le zelo kratek čas in jih izbrisati takoj, ko potnik prečka kontrolno točko.

C.3.6 Če se za vpis uporablja aplikacija, med razvojem aplikacije uporabljati varnostne standarde za varnost mobilnih aplikacij, pa tudi varnostne preskuse, ki jih opravi tretja oseba.

C.3.7 Zagotoviti, da so v fazi vpisa na letališču vzpostavljeni varnostni ukrepi za ohranitev zaupnosti in celovitosti biometričnih podatkov potnika. Če terminal na primer natisne kodo QR, ta v njem ne sme biti prikazana, da bi preprečili, da bi jo zlonamerni akter fotografiral. Pri prenosih na kratke razdalje mora dejavno sodelovati uporabnik, izvajati pa se morajo prek kanala, ki zagotavlja bližino.

C.3.8 Podatke, ki so izključno v lasti posameznika[82], je treba hraniti v varnem pomnilniku na napravi posameznika, na vseh morebitnih šibkih točkah, povezanih z operacijskimi sistemi naprave, pa si je treba namestiti ustrezne varnostne popravke. Če je koda QR natisnjena, je treba posameznika seznaniti s posebno občutljivo naravo podatkov, ki jih vsebuje, in s tem, kaj omogoča.

C.3.9 Zagotoviti, da se vpis izvede v skladu z ustreznimi tehnikami za preverjanje identitete na daljavo[83].

3.2.2 Scenarij 2: centralizirana hramba vpisane biometrične predloge za avtentikacijo v šifrirani obliki na letališču in s ključem oziroma skrivnim podatkom, ki ga poznajo le potniki

48. V tem oddelku je preučeno, ali je centralizirana hramba biometričnih predlog potnikov, ki se uporabljajo za avtentikacijo, v centralizirani podatkovni zbirki v šifrirani obliki in s ključem oziroma skrivnim podatkom, ki ga pozna le potnik, združljiva s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov [84] (v nadaljevanju: **scenarij 2**). V tem oddelku so preučeni tudi ustrezni zaščitni ukrepi za scenarij 2 v skladu s 25. in 32. členom Splošne uredbe o varstvu podatkov.

Opis scenarija

49. V scenariju 2 se vpis opravi le enkrat za določeno obdobje veljavnosti (na primer eno leto po zadnjem letu do izteka obdobja veljavnosti potnega lista) na daljavo na ustrezni ravni zanesljivosti identitete (na primer raven zanesljivosti, ki ustreza ravni po uredbi eIDAS) ali na letaliških terminalih. Vpis nadzoruje upravljavec letališča, zajema pa generiranje identifikacijskih in biometričnih podatkov, ki so šifrirani s ključem oziroma skrivnim podatkom.

50. Podatkovna zbirka se hrani v prostorih letališča pod nadzorom upravljavca letališča. Posamezni posebni šifrirni ključi oziroma skrivni podatki se hranijo le na napravi posameznika (na primer v mobilni

[82] Sklici na biometrično predlogo v zaščitnih ukrepih v scenariju 1 ustrezajo sklicem na ključ oziroma skrivni podatek v scenariju 2.
[83] Glej poročilo agencija ENISA o preverjanju identitete na daljavo: analiza metod za preverjanje identitete na daljavo, marec 2021.
[84] Kot je ponazorjeno s primerom uporabe 2 v Prilogi I k zahtevku.

aplikaciji upravljavca letališča). Aplikacija lahko generira kodo QR, ki vsebuje ključ oziroma skrivni podatek, ki se lahko natisne na papir ali prikaže na zaslonu naprave[85]. Upravljavec letališča poleg tega izvede drugo raven šifriranja[86] s ključi, ki so pod njegovim nadzorom.

51. Potniki se avtenticirajo (primerjava „ena proti ena“), ko gredo skozi posamezne kontrolne točke na letališču. Potniki, ki se odločijo za prehod skozi biometrične kontrolne točke, pokažejo kodo QR pri namenskem kontrolnem terminalu, opremljenem z optičnim bralnikom kod QR in kamero. Indeks potnika se pošlje v podatkovno zbirko, da se zahteva šifrirana predloga, ki se prenese in preveri lokalno na terminalu in/ali napravi uporabnika. Kontrolor na kontrolni točki pozna in uporablja le rezultat ugotavljanja ujemanja[87].

52. V tem scenariju ni pretoka identifikacijskih in biometričnih podatkov med letališči, centralizirane podatkovne zbirke pa niso niti povezane niti interoperabilne.

Ocena EOVP

53. V scenariju 2 se vpisane biometrične predloge potnikov hranijo centralizirano, vendar v šifrirani obliki in s ključem oziroma skrivnim podatkom, ki ga pozna le potnik. V scenariju 2 se potniki avtenticirajo (primerjava „ena proti ena“).

54. V tem scenariju se predlaga, da bi lahko cilj pospešitve pretoka potnikov (tj. s hitrejšimi pregledi), dosegli z uporabo centraliziranega sistema. EOVP je že prej navedel, da bi lahko bila taka rešitev izvedljiva alternativa decentralizirani hrambi vpisanih biometričnih predlog[88] (kot je opisano v scenariju 1), če obstajajo objektivne potrebe in se uporabljajo ustrezni zaščitni ukrepi (glej zaščitne ukrepe, opisane v nadaljevanju v točki 60).

55. Z vidika varnosti so podatki vsakega posameznika šifrirani s posebnim ključem, ki ga pozna le posameznik in je pod njegovim izključnim nadzorom. Poleg tega dejstvo, da mora posameznik navesti informacije, potrebne za ugotavljanje ujemanja (tj. skrivni podatek oziroma ključ), deluje kot drug dejavnik[89] in tako krepi varnost avtentikacije. Upravljavec letališča poleg tega izvede drugo raven šifriranja s ključi, ki so pod njegovim nadzorom. V scenariju 2 se indeks posameznika pošlje v osrednjo podatkovno zbirko, da se pridobijo z njim povezani biometrični podatki. Ti podatki se nato (šifrirani) pošljejo v računalnik na kontrolni točki, kjer se dešifrirajo, da se ugotovi ujemanje, kontrolor na kontrolni točki pa pozna in uporablja samo rezultat ugotavljanja ujemanja. Če se ključ oziroma skrivni podatek posameznika hrani v računalniku, ki je na kontrolni točki, in če se v osrednjo podatkovno zbirko za obnovitev šifrirane biometrične predloge pošlje le indeks potnika, bi se lahko taki varnostni ukrepi šteli za združljive s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov.

---

[85] Francoski nadzorni organ je nadalje pojasnil, da morda obstajajo tudi druge tehnične rešitve za pošiljanje zahtevanih informacij, na primer z uporabo komunikacijskega protokola kratkega dosega.

[86] Ključ oziroma skrivni podatek (ki ga pozna posameznik) je šifriran z drugim ključem, ki ga pozna upravljavec letališča.

[87] Francoski nadzorni organ je pojasnil, da je to obdobje hrambe le za ponazoritev in se lahko šteje za sprejemljivo, saj ključ poznajo le posamezniki in se lahko izbere v fazi vpisa. Vendar je treba opozoriti, da se lahko tako obdobje hrambe prilagodi.

[88] Smernice EOVP 3/2019 o video napravah, točka 88.

[89] S tem se na primer zmanjša tveganje za slepljenje identitete. Glej tudi varnostni ukrep C.1.2.

56. Glede združljivosti s 25. členom Splošne uredbe o varstvu podatkov in zlasti za izpolnitev zahteve glede najmanjšega obsega podatkov je treba zagotoviti, da obdelava izpolnjuje načelo potrebnosti. V scenariju 2 bi se lahko štelo, da izbrani ukrepi izpolnjujejo načelo potrebnosti glede na predvideni namen (tj. pospešiti pretok potnikov na letališčih), če lahko upravljavec glede na okoliščine obdelave dokaže, da ni alternativnih rešitev, ki manj posegajo v zasebnost, s katerimi bi se lahko enako učinkovito dosegel isti cilj. V scenariju 2 bi potniki še vedno morali pokazati svojo napravo[90]. Upravljavec pa lahko kljub temu dokaže, da se s scenarijem 2 pospeši postopek preverjanja v primerjavi s sedanjim stanjem, pri katerem preverjanje, ki ga opravijo ljudje, zajema ugotavljanje, ali se ime na vstopnem kuponu ujema z osebnim dokumentom potnika[91], ali ko se primerja s scenarijem 1. Tega zlasti ne bi bilo mogoče dokazati, če se trenutno ne preverja identiteta potnikov na podlagi njihovega uradnega osebnega dokumenta (glede tega glej točko 18 zgoraj).

57. Kar zadeva načelo sorazmernosti, se lahko poseganje v zasebnost pri taki obdelavi uravnoteži z dejavnim sodelovanjem potnikov, ki imajo pod izključnim nadzorom ključ do svojih šifriranih podatkov. Poleg tega se zdi, da je mogoče varnostna tveganja, povezana s hrambo biometričnih podatkov potnikov v centralizirani podatkovni zbirki in s ključem, ki ga pozna le potnik, zmanjšati z uporabo ustreznih zaščitnih ukrepov (glej zaščitne ukrepe, obravnavane v nadaljevanju v točki 60). Če bi upravljavec izvajal ustrezne zaščitne ukrepe, kot se zahtevajo z zadevno posebno obdelavo, bi se tako lahko tveganja za posameznike zmanjšala, negativni vpliv na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, pa bi se lahko obravnaval kot sorazmeren s pričakovano koristjo. Seveda bi bilo treba v vsakem primeru zagotoviti, da se obdelujejo le podatki, potrebni za ta namen, in da se preverjajo le potniki, ki so v to privolili, zato ni tveganja, da bi se zbirali biometrični podatki drugih potnikov, ki v to niso privolili.

58. V zahtevku je kot primer navedeno, da je lahko v scenariju 2 obdobje hrambe šifriranih podatkov v podatkovni zbirki običajno eno leto po zadnjem letu posameznika in do izteka obdobja veljavnosti potnega lista. V zahtevku niso bile predložene informacije, s katerimi bi se utemeljilo tako dolgo obdobje na podlagi objektivnih razlogov, čeprav je mogoče domnevati, da je tako obdobje hrambe predvideno, ker je to pripravno za prihodnje lete. Da bi se v tem scenariju dosegla skladnost s točko e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov, bi morali biti upravljavci glede obdobja hrambe zmožni utemeljiti, zakaj je v posebnih primerih za ta namen potrebno tako obdobje hrambe. EOVP upravljavcem priporoča, naj predvidijo najkrajše možno obdobje hrambe, pri čemer naj upoštevajo tudi potnike, ki letijo zelo redko, in posameznikom, na katere se nanašajo osebni podatki, ponudijo možnost, da določijo želeno obdobje hrambe.

59. EOVP ob upoštevanju teh premislekov v odgovoru na vprašanje 2.1.1 ugotavlja, da bi se **lahko načeloma štelo**, da je taka obdelava **združljiva s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov, če bi se izvajali ustrezni zaščitni ukrepi**.

Ustrezni zaščitni ukrepi

[90] Francoski nadzorni organ je dodatno pojasnil, da bi se lahko predloga predložila tudi drugače, na primer natisnjena na papirju. Poleg tega EOVP priznava, da bi se lahko v prihodnosti predvidela uporaba alternativne tehnologije, na primer na podlagi komunikacijskega sistema v bližnjem polju.

[91] Lahko bi tudi trdili, da so napake pri biometričnem preverjanju manj verjetne kot pri preverjanju, ki ga opravijo ljudje.

60. EOVP v tovrstnem scenariju v odgovoru na vprašanje 2.1.2 meni, da bi bilo treba **poleg zaščitnih ukrepov iz scenarija 1** izvajati vsaj naslednje zaščitne ukrepe. *Za doseganje istih ciljev glede varnosti in varstva podatkov bi se lahko poleg zaščitnih ukrepov, opisanih v tem mnenju, uporabili tudi drugi zaščitni ukrepi, ki bi bili zakoniti, če bi zagotavljali skladnost z veljavnimi pravnimi okviri.*

61. Opomba: *to je neizčrpen pregled morebitnih ustreznih zaščitnih ukrepov na visoki ravni, ki bi jih upravljavec lahko izvajal pri rešitvi, podobni scenariju 2. Njihova ustreznost v skladu s 25. in 32. členom Splošne uredbe o varstvu podatkov bo odvisna od analize posameznih primerov. Vsi upravljavci bodo morali zagotoviti, da bodo izvedli lastno oceno učinka v zvezi z varstvom podatkov, zaradi njihovih posebnih rešitev pa bi lahko bili potrebni dodatni ukrepi, ki v to mnenje niso vključeni.*

D. Splošni

D.1 Pravice posameznikov in zaščitni ukrepi, ki jih lahko izvajajo upravljavci

D.1.1 Zagotoviti, da ima potnik nadzor nad obdobji hrambe vseh svojih podatkov. Obdobja hrambe bi morala biti omejena na to, kar je potrebno za poseben namen. Najdaljše obdobje bi bilo treba določiti na podlagi temeljite analize dejavnikov, kot je obdobje veljavnosti identifikacijskega dokumenta. Posameznikom bi bilo treba ponuditi možnost, da določijo želeno obdobje hrambe, ki bi lahko bilo krajše od privzetega.

D.1.2 Omogočiti posamezniku, da kadar koli zahteva izbris podatkov, ki jih pozna le on (ključ oziroma skrivni podatek), kot se hranijo v mobilni aplikaciji ali digitalni denarnici[92].

D.1.3 Zagotoviti, da lahko pristojni nadzorni organ učinkovito nadzoruje krajevno prilagoditev osrednje podatkovne zbirke.

E. Organizacijski:

E.1 Politika in skladnost

E.1.1 Zaupanje v centralni strežnik mora biti omejeno. Zagotoviti, da upravljanje centralnega strežnika poteka v skladu z jasno opredeljenimi pravili upravljanja in vključuje vse potrebne ukrepe za zagotovitev njegove varnosti[93].

F. Tehnični:

F.1 Dostop

F.1.1 Voditi dnevnike o tem, kdo ima dostop do osebnih podatkov, zlasti identifikacijskih in biometričnih podatkov, ter kdaj je bil dostop omogočen.

[92] Upoštevajte, da ta zaščitni ukrep velja samo za scenarij 2.
[93] Smernice EVOP št. 04/2020 o lokacijskih podatkih in orodjih za sledenje stikom, PRIV-5, str. 17.

F.2 Infrastruktura in omrežje

F.2.1 Ustrezno zavarovati osrednjo podatkovno zbirko, tudi pred napadi, ki vplivajo na razpoložljivost.

F.2.2 Zagotoviti, da ni internetne povezave z osrednjo podatkovno zbirko, vpisnimi terminali in enotami za ugotavljanje ujemanja. Delovanje in vzdrževanje teh sistemov (na primer varnostno kopiranje, nameščanje popravkov, spremljanje itd.) je treba izvajati lokalno v prostorih letališča.

F.3 Varnost in upravljanje podatkov

F.3.1 Uporabiti najnovejše kriptografske tehnike, da se zavarujejo izmenjave med aplikacijo in centraliziranim strežnikom[94].

F.3.2 Posamezni ključ oziroma skrivni podatek hraniti na ravni, na kateri se bo uporabljal za dešifriranje (tj. na terminalu), indeks pa uporabiti samo za obnovitev ustrezne vpisane biometrične predloge v osrednji podatkovni zbirki.

F.3.3 Zagotoviti, da izmenjava ključa oziroma skrivnega podatka med napravo uporabnika in terminalom varuje komunikacijo pred morebitnim prisluškovanjem ali prenosom tretjim osebam.

F.3.4 Indeksirati biometrično predlogo, ko se shrani v osrednjo podatkovno zbirko, da se omogoči avtentikacija „ena proti ena“ ter zagotovi, da je edinstvena in povezana s posameznikom. Zagotoviti, da indeks ne razkriva identifikacijskih podatkov potnika in ni povezan s šifrirnim ključem.

F.3.5 Ustrezno avtenticirati in šifrirati vsak prenos med osrednjo podatkovno zbirko in kontrolnimi točkami ter ga namestiti na izolirana omrežja.

F.3.6 Izogibati se dvosmernim povezavam med nabori podatkov (identifikacijski in biometrični podatki ter podatki o letu) in v podatkovni zbirki hraniti le ustrezne enosmerne povezave. Na primer le enosmerne povezave od indeksa do identifikacijskih podatkov, od indeksa do šifriranih biometričnih podatkov in od indeksa do podrobnosti o letu.

F.3.7 Zagotoviti ureditev neprekinjenega poslovanja, na primer z vzpostavitvijo ustreznih sistemov za varnostno shranjevanje.

[94] Smernice EOVP št. 04/2020 o lokacijskih podatkih in orodjih za sledenje stikom, SEC-4, str. 16: „Primeri tehnik, ki se lahko uporabijo, so: simetrično in asimetrično šifriranje, zgoščevalne funkcije (*hash functions*), šifrirni protokoli PMT (*private membership test*), PSI (*private set intersection*) in PIR (*private information retrieval*), Bloomovi filtri, homomorfno šifriranje itd.“

F.3.8 Zagotoviti, da se na terminalu ne vodijo dnevniki šifriranih ali nešifriranih predlog.

3.2.3 Centralizirana hramba vpisanih biometričnih predlog za identifikacijo

62. V tem oddelku je preučeno, ali je centralizirana hramba vpisanih biometričnih predlog potnikov za identifikacijo združljiva s točkama e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov, če take predloge niso šifrirane s ključem oziroma skrivnim podatkom, ki ga pozna le potnik, v dveh primerih uporabe: (1.) če se take predloge hranijo v podatkovni zbirki na letališču pod nadzorom upravljavca letališča[95] (v nadaljevanju: **scenarij 3.1**) in (2.) če se take predloge hranijo v oblaku pod nadzorom letalske družbe[96] (v nadaljevanju: **scenarij 3.2**).

63. EOVP meni, da uporaba biometričnih podatkov za **identifikacijske** namene v velikih osrednjih podatkovnih zbirkah posega v temeljne pravice posameznikov, na katere se nanašajo osebni podatki, in bi lahko imela zanje resne posledice[97]. Poleg tega bi bilo treba uporabo biometričnih podatkov preučiti tudi glede na namen, za katerega se obdelujejo, pri tem pa upoštevati načeli potrebnosti in sorazmernosti[98].

3.2.3.1 Scenarij 3.1: centralizirana hramba v podatkovni zbirki na letališču, ki je pod nadzorom upravljavca letališča

Opis scenarija

64. V scenariju 3.1 se vpisana biometrična predloga potnikov v šifrirani obliki hrani v osrednji podatkovni zbirki v prostorih letališča in je pod nadzorom upravljavca letališča. Podatki o potnikih so razdeljeni, kar zlasti pomeni, da se njihovi identifikacijski podatki, vpisana biometrična predloga in podatki o letu hranijo v treh različnih podatkovnih zbirkah. Ti podatki so šifrirani z različnimi ključi, tako med hrambo kot tudi med prenosom na strežnike, na katerih se izvaja ugotavljanje ujemanja, kjer jih nato dešifrira upravljavec letališča.

65. Potniki se morajo na vsak let prijaviti ne dolgo pred odhodom (na primer 48 ur). Tak vpis se lahko izvede na daljavo ali na letaliških terminalih na ustrezni ravni zanesljivosti identitete (na primer raven zanesljivosti, ki ustreza ravni po uredbi eIDAS). Druga možnost je, da vpis poteka enako, kot je opisano v scenariju 1, v tem primeru pa morajo potniki v 48 urah pred odhodom prenesti svoje podatke iz digitalnih denarnic v letališki sistem.

66. Tudi v tem scenariju gredo potniki v namenski kontrolni terminal, opremljen s kamero. Njihov biometrični vzorec se nato pošlje centralnemu strežniku letališča, ki bo poskušal ugotoviti ujemanje teh podatkov s podatki iz osrednje biometrične podatkovne zbirke. Tako je mogoče potnika identificirati in preveriti, ali je dejansko registriran za odhodni let (ali za let, za katerega poteka vkrcanje, v primeru kontrole pri vkrcanju). Podatki, ki se pošljejo nazaj upravljavcu kontrolne točke, ki

[95] Kot je ponazorjeno s primerom uporabe 3A v Prilogi I k zahtevku.
[96] Kot je ponazorjeno s primerom uporabe 3B v Prilogi I k zahtevku.
[97] Glej na primer Mnenje delovne skupine iz člena 29 št. 3/2012 o biometričnih tehnologijah, str. 8. Glej tudi točko 26.
[98] Uvodna izjava 4 Splošne uredbe o varstvu podatkov. Glej tudi Mnenje delovne skupine iz člena 29 št. 3/2012 o biometričnih tehnologijah, str. 8.

vloži zahtevo, se lahko glede na kontrolno točko zmanjšajo na najmanjši obseg, na primer kot odgovor „da/ne“ ali po potrebi kot rezultat ugotavljanja ujemanja. V tem primeru se upravljavcu kontrolne točke posreduje in ta uporablja le rezultat zahteve.

67. V tem scenariju se zlasti potniki identificirajo (primerjava „ena proti N“), pri čemer je N število potnikov, pričakovanih na letališču v časovnem okviru več dni. Poleg tega se ugotavljanje ujemanja biometričnih podatkov izvede le, ko se vsak potnik prijavi na vnaprej določenih kontrolnih točkah na letališču odhoda, obdelava podatkov pa poteka na centralnem strežniku, povezanem z osrednjo podatkovno zbirko. Obdobje hrambe v tem scenariju je običajno 48 ur, podatki pa se izbrišejo, ko letalo vzleti.

Ocena EOVP

68. Kot je navedeno zgoraj, obdelava biometričnih podatkov pomeni večja tveganja za pravice in svoboščine posameznikov[99]. Zato ima lahko vsaka kršitev varstva podatkov posebno resne posledice za posameznike[100]. Upravljavci morajo ta tveganja učinkovito zmanjšati. Ker je po tem scenariju celotna arhitektura povsem centralizirana, potniki bolj izgubijo nadzor nad svojimi podatki. Poleg tega bi se lahko tudi povečalo tveganje, da bi se podatki obdelovali za druge namene, ki niso povezani z nadzorom pretoka potnikov.

69. Ob upoštevanju načela in zahtev glede varnosti (točka f prvega odstavka 5. člena in 32. člen Splošne uredbe o varstvu podatkov) je treba upoštevati, da lahko hramba identifikacijskih in biometričnih podatkov v osrednjih, čeprav ločenih podatkovnih zbirkah pomeni točko napada visoke vrednosti, s kršitvijo zaupnosti take podatkovne zbirke pa se lahko nato omogoči dostop do celotnega nabora podatkov. Zaradi morebitne kršitve, ki se nanaša na predloge za prepoznavanje obrazov in povezane identifikacijske podatke, je posledično mogoče posameznike v drugih okoljih nepooblaščeno ali nezakonito identificirati. Glede na uporabljene metode biometrične identifikacije lahko tudi ogrozi nadaljnjo varno uporabo predlog za prepoznavanje obrazov kot identifikatorja. V tem primeru ni mogoče zmanjšati učinkov kršitve v nasprotju z drugo vrsto poverilnic (na primer ID uporabnika, geslo), ki jih je mogoče spremeniti[101].

70. Poleg tega je zaradi velike količine ter kakovosti identifikacijskih in biometričnih podatkov, ki jih hrani upravljavec, le ta zelo dragocena tarča napadalcev, kar pomeni večjo verjetnost z vidika varnostnega tveganja. Poleg tega bi lahko imele kršitve varstva podatkov večji vpliv, saj bi lahko napadalci zaradi hrambe podatkov na centralizirani lokaciji lažje pridobili dostop do osebnih podatkov več potnikov. Z morebitno kršitvijo bi se zato lahko veliko posameznikov izpostavilo zelo resnemu velikemu tveganju, na primer obsežni kraji identitete, ki ga je zelo težko zmanjšati.

71. Ukrepi iz scenarija 3.1[102], kar zadeva združljivost s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov, pri čemer se upošteva najnovejši tehnološki razvoj, zato

[99] Glej točko 26.

[100] *Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data* (smernice o prepoznavanju obrazov Posvetovalnega odbora Konvencije Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov), junij 2021, str. 22.

[101] Glej v zvezi s tem Mnenje delovne skupine iz člena 29 št. 3/2012 o biometričnih tehnologijah, str. 34.

[102] Kot je navedeno v točkah 64 do 67.

ne zadostujejo za zagotovitev ravni varnosti, ki ustreza tveganju. Na podlagi tega obdelava v skladu s scenarijem 3.1 ne bi bila v skladu s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov, če bi se upravljavec omejil na navedene ukrepe.

72. Ob upoštevanju načela iz točke e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov je v tem scenariju obdobje hrambe biometričnih podatkov v osrednji podatkovni zbirki običajno 48 ur. Zdi se, da se s tako omejitvijo hrambe znatno zmanjšuje tveganje, povezano s kršitvami varstva osebnih podatkov. Obdobje hrambe podatkov pa samo po sebi ni odločilen dejavnik za splošno združljivost navedene arhitekture, saj lahko upravljavci taka obdobja hrambe spremenijo. Predlagani ukrepi morajo vsekakor izpolnjevati zahteve glede vgrajenega in privzetega varstva podatkov iz 25. člena Splošne uredbe o varstvu podatkov.

73. V nasprotju s scenarijema 1 in 2, pri katerih se potniki avtenticirajo, se potniki v scenariju 3.1 identificirajo (primerjava „ena proti N“), pri čemer je N število potnikov, ki se pričakujejo na letališču v časovnem okviru več dni in ki privolijo v tako obdelavo, ko gredo skozi posamezne kontrolne točke na letališču. To pomeni iskanje potnikov v osrednji podatkovni zbirki z obdelavo vsakega zajetega biometričnega vzorca, da se preveri, ali se ugotovi ujemanje z osebo, ki jo sistem pozna. V scenariju 3.1 v nasprotju s scenarijem 2 ključev ne poznajo le potniki. Zato imajo ti po tem scenariju bistveno manjši nadzor nad svojimi biometričnimi podatki. Obdelava, kot je predlagana v scenariju 3.1, torej ne more biti združljiva z zahtevami glede vgrajenega in privzetega varstva podatkov iz 25. člena Splošne uredbe o varstvu podatkov.

74. Glede na 25. člen Splošne uredbe o varstvu podatkov bi morali upravljavci upoštevati vrste, kategorije in raven podrobnosti osebnih podatkov, potrebnih za namene obdelave[103]. Pri svojih odločitvah glede oblikovanja bi morali upoštevati čedalje večja tveganja za načela najmanjšega obsega podatkov, celovitosti in zaupnosti ter omejitve hrambe pri zbiranju velikih količin podrobnih osebnih podatkov ter jih primerjati z manjšimi tveganji pri zbiranju manjših količin in/ali manj podrobnih informacij o posameznikih, na katere se nanašajo osebni podatki. Vsekakor pa privzeta nastavitev ne bi smela vključevati zbiranja osebnih podatkov, ki niso potrebni za določen namen obdelave. Z drugimi besedami, če so posamezne kategorije osebnih podatkov nepotrebne ali če podrobni podatki niso potrebni, ker zadostujejo manj podrobni podatki, se dodatni osebni podatki ne bi smeli zbirati. Če bi bilo mogoče z drugim postopkom obdelave doseči isti cilj in bi bil na voljo v skladu s pogoji, opisanimi v scenariju 3.1, v tem primeru ne bi bilo treba uporabljati tehnologije za prepoznavanje obrazov.

75. Kar zadeva 25. člen Splošne uredbe o varstvu podatkov, je ključni element vgrajenega in privzetega varstva podatkov samostojnost posameznika, na katerega se nanašajo osebni podatki. Posameznikom, na katere se nanašajo osebni podatki, je treba zagotoviti najvišjo možno stopnjo samostojnosti pri določanju uporabe svojih osebnih podatkov ter glede obsega in pogojev te uporabe ali obdelave[104]. V scenariju 1 bi se posamezniku, na katerega se nanašajo osebni podatki, zagotovila samostojnost in nadzor nad uporabo, razkritjem in izbrisom biometričnih predlog, v scenariju 2 pa bi ohranil določen nadzor v zvezi z razkritjem biometrične predloge, saj bi hranil šifrirni ključ oziroma skrivni podatek. V scenariju 3.1 pa je posameznik, na katerega se nanašajo osebni podatki, glede obdelave svojih

[103] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 49.

[104] Smernice EOVP št. 4/2019 o členu 25 Vgrajeno in privzeto varstvo podatkov, točka 70. V uvodni izjavi 7 splošne uredbe o varstvu podatkov je nadalje pojasnjeno, da bi „[p]osamezniki [...] morali imeti nadzor nad lastnimi osebnimi podatki“.

biometričnih podatkov povsem odvisen od odločitev upravljavca, zato nima neposrednega nadzora nad uporabo svoje biometrične predloge.

76. Kar zadeva združljivost s 25. členom Splošne uredbe o varstvu podatkov in zlasti da se izpolni zahteva glede najmanjšega obsega podatkov, obdelava iz scenarija 3.1 ne more izpolnjevati načela potrebnosti. EOVP meni, da je mogoče podoben rezultat, kakršen se doseže s pospešitvijo pretoka potnikov na letališčih, doseči na način, ki manj posega v zasebnost. To je na primer mogoče doseči brez uporabe biometričnih podatkov (čeprav bi bila izkušnja uporabnika v tem primeru drugačna, saj bi lahko trajalo dlje časa, da se pokažejo vstopni kupon in po potrebi uradni identifikacijski dokumenti). Poleg tega druge rešitve, zlasti tiste, ki temeljijo na lokalni hrambi biometričnih podatkov v denarnici na napravi posameznika, ali tiste, pri katerih je treba podatke šifrirati s posebnim ključem, ki se hrani v napravi posameznika, omogočajo, da se cilji dosežejo na način, ki manj posega v zasebnost.

77. Kar zadeva načelo sorazmernosti, bi obdelava iz scenarija 3.1 povzročila tveganja za pravice posameznikov, na katere se nanašajo osebni podatki, ki se s predvidenimi ukrepi glede na najnovejši tehnološki razvoj ne bi zmanjšala. Zdi se, da tveganje negativnega vpliva na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ki bi lahko bil posledica kršitve varstva podatkov v centralizirani podatkovni zbirki biometričnih podatkov velikega števila posameznikov, prevlada nad pričakovano koristjo, ki izhaja iz obdelave, saj je ta razmeroma majhna, tj. malo prijetnejši in hitrejši pregledi. Zato ne more upravičiti tega, da ti ukrepi zelo posegajo v temeljne pravice in svoboščine posameznikov, obdelava iz scenarija 3.1 pa ni v skladu z načelom sorazmernosti.

78. EOVP ob upoštevanju teh premislekov v odgovoru na vprašanje 2.2.1 ugotavlja, da kadar se obdelava izvaja za namen pospešitve pretoka potnikov na letališčih, obdelava iz scenarija 3.1:

- **ne more biti združljiva s 25. členom Splošne uredbe o varstvu podatkov ter**
- **ne bi bila v skladu s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov,** če bi se upravljavec omejil na ukrepe, opisane v scenariju 3.1.

3.2.3.2 Scenarij 3.2: Centralizirana hramba v oblaku, ki je pod nadzorom letalske družbe

Opis scenarija

79. V scenariju 3.2 se vpisana biometrična predloga potnikov shrani v oblaku pod nadzorom letalske družbe ali njenega ponudnika storitev v oblaku (obdelovalca podatkov). V zahtevku je navedeno, da bi imel ponudnik storitev v oblaku sedež v EGP[105]. V tem primeru so podatki o potnikih šifrirani, vendar se dešifrirajo, ko so v uporabi (na primer ob izvedbi postopka ugotavljanja ujemanja), ključe pa nadzoruje letalska družba ali njen obdelovalec v oblaku. Biometrični podatki potnikov se uporabljajo za identifikacijo potnikov (primerjava „ena proti N“), pri čemer je N lahko enako številu vseh strank letalske družbe[106].

80. Potniki se morajo podobno kot v scenarijih 1, 2 in 3.1 tudi v tem scenariju najprej vpisati. Vendar se v scenariju 3.2 vpis potnikov opravi enkrat, dokler ima stranka račun pri letalski družbi. Vpis se opravi na daljavo na ustrezni ravni zanesljivosti identitete (na primer raven zanesljivosti, ki ustreza ravni po uredbi eIDAS) ali na letaliških terminalih. Ugotavljanje ujemanja biometričnih podatkov se izvede le, ko se potniki prijavijo na vnaprej določenih kontrolnih točkah na letališču, obdelava podatkov pa poteka v oblaku.

81. Na letališču gredo potniki skozi namenske kontrolne terminale, opremljene s kamero. Biometrični podatki potnikov se na zahtevo pošljejo letalskemu prevozniku v strežnik v oblaku, kjer se izvaja ugotavljanje ujemanja teh podatkov in podatkov iz centralne podatkovne zbirke. Tako je mogoče potnika identificirati in preveriti, ali je dejansko registriran za odhodni let (ali za let, za katerega poteka vkrcanje, v primeru kontrole pri vkrcanju).

82. Rezultati ugotavljanja ujemanja se lahko po možnosti dajo na voljo več upravljavcem letališč, če ima letalska družba namenski terminal ali dostop do infrastrukture skupnega informacijskega sistema letališča. Podatki, ki se pošljejo nazaj upravljavcu kontrolne točke, ki vloži zahtevo, se lahko glede na kontrolno točko zmanjšajo na najmanjši obseg, na primer kot odgovor „da/ne“ ali po potrebi rezultat ugotavljanja ujemanja. V tem primeru kontrolor na kontrolni točki pozna in uporablja le rezultat zahteve.

83. Obdobje hrambe predloge določi letalska družba in lahko traja dokler ima stranka račun pri letalski družbi.

Ocena EOVP

84. Premisleki, ki jih je EOVP že izrazil v zvezi s scenarijem 3.1[107], veljajo tudi za ta scenarij.

85. Kar zadeva načelo in zahteve glede varnosti (točka f prvega odstavka 5. člena in 32. člen Splošne uredbe o varstvu podatkov), se obdelava iz scenarija 3.2 izvaja v oblaku, do takih podatkov pa bi lahko imelo dostop več subjektov, vključno z morebitnimi ponudniki zunaj EGP, tudi če se podatki hranijo v

[105] Francoski nadzorni organ je pojasnil, da gre za ponazoritev in da bi se lahko upoštevali tudi ponudniki storitev v oblaku, ki nimajo sedeža v EGP. Poleg tega bi lahko predvideli tudi druge rešitve za hrambo (na primer brez uporabe oblaka).
[106] Francoski nadzorni organ je pojasnil, da gre za ponazoritev in da obstaja rešitev, po kateri se biometrični podatki posredujejo vsakič pred letom.
[107] Točke 68 do 77.

EGP[108]. Taka arhitektura vključuje morebitna tveganja v zvezi s prenosi osebnih podatkov v tretje države. Čeprav so podatki o potnikih šifrirani, se dešifrirajo, ko so v uporabi (tj. ob izvedbi postopka ugotavljanja ujemanja), ključe pa nadzoruje letalska družba ali njen obdelovalec v oblaku. Zaradi take hrambe bi se lahko še povečal obseg varnostne izpostavljenosti.

86. Kar zadeva združljivost s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov, ukrepi iz scenarija 3.2[109], pri čemer se upošteva najnovejši tehnološki razvoj, zato ne zadostujejo za zagotovitev ravni varnosti, ki ustreza tveganju. Na podlagi tega obdelava v skladu s scenarijem 3.2 ne bi bila v skladu s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov, če bi se upravljavec omejil na navedene ukrepe.

87. Poleg tega bi se lahko podatki v skladu s scenarijem 3.2[110] hranili daljše obdobje (tj. po možnosti tako dolgo, dokler ima posameznik račun pri letalski družbi). S tako dolgim obdobjem hrambe so podatki izpostavljeni večjemu tveganju kršitve njihove zaupnosti in celovitosti ter se presega to, kar je nujno potrebno in sorazmerno za namene obdelave. EOVP ugotavlja, da obdobje hrambe podatkov samo po sebi ni odločilno za splošno združljivost navedene strukture s Splošno uredbo o varstvu podatkov, saj ga lahko upravljavci podatkov spremenijo. Na podlagi informacij, ki so na voljo EOVP in so navedene v opisu scenarija 3.2, ni zadostne utemeljitve za to dolgo obdobje hrambe in ni očitnih ukrepov za zmanjšanje tveganj za posameznike. Na podlagi tega predlagano obdobje hrambe ne bi bilo omejeno na to, kar je potrebno, kot to določa načelo omejitve hrambe iz točke e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov.

88. Predlagani ukrepi iz scenarija 3.2 vsekakor ne morejo izpolnjevati zahtev glede vgrajenega in privzetega varstva podatkov iz 25. člena Splošne uredbe o varstvu podatkov. V scenariju 3.2 se biometrične predloge potnikov hranijo v oblaku, ki je pod nadzorom letalske družbe ali njenega ponudnika storitev v oblaku (obdelovalec podatkov). Kot je opisano zgoraj, bi lahko imelo dostop do teh podatkov več subjektov. Poleg tega se biometrični podatki potnikov uporabljajo za identifikacijo potnikov (primerjava „ena proti N“), pri čemer je N lahko enako številu vseh uporabnikov oziroma strank letalske družbe. Taka metoda vključuje iskanje osebe med skupinami posameznikov v osrednji podatkovni zbirki z obdelavo vsakega zajetega obraza, da se preveri, ali se ugotovi ujemanje z osebo, ki jo sistem pozna. V nasprotju s scenarijem 3.1 bi se lahko primerjava v scenariju 3.2 izvedla v veliko večjem obsegu, saj je merilo v tem primeru število vseh strank letalske družbe, v scenarij 3.1 pa je vključeno le število potnikov, pričakovano v časovnem okviru več dni.

89. Poleg tega, kar zadeva združljivost s 25. členom Splošne uredbe o varstvu podatkov in zlasti da se izpolni zahteva glede najmanjšega obsega podatkov, obdelava iz scenarija 3.2 ne more izpolnjevati načela potrebnosti. EOVP meni, da bi bilo mogoče podoben rezultat, kakršen se doseže s pospešitvijo pretoka potnikov na letališčih, doseči z drugimi ukrepi, ki manj posegajo v zasebnost, na primer brez uporabe biometričnih podatkov, čeprav bi bila izkušnja uporabnika v tem primeru drugačna, saj bi lahko trajalo dlje časa, da pokažejo osebno izkaznico in vstopni kupon. Poleg tega druge rešitve, zlasti tiste, ki temeljijo na lokalni hrambi biometričnih podatkov v denarnici na napravi posameznika, ali

[108] EOVP 2022, *Coordinated Enforcement Action on the use of cloud-based services by the public sector* (usklajeni izvršilni ukrepi v zvezi z uporabo storitev v oblaku v javnem sektorju) z dne 17. januarja 2023, str. 19.
[109] Glej točke 79 do 83.
[110] Glej točko 83.

tiste, pri katerih je treba podatke šifrirati s posebnim ključem, ki se hrani v napravi posameznika, upravljavcu omogočajo, da cilje doseže na način, ki manj posega v zasebnost.

90. Kar zadeva načelo sorazmernosti, bi obdelava iz scenarija 3.2 povzročila tveganja za pravice posameznikov, ki se s predvidenimi zaščitnimi ukrepi ne bi zmanjšala. Zdi se, da negativni vpliv na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ki bi bil posledica kršitve varstva podatkov v centralizirani podatkovni zbirki biometričnih podatkov velikega števila posameznikov, ki se hranijo v oblaku, prevlada nad pričakovano koristjo, ki izhaja iz obdelave, saj je ta razmeroma majhna, tj. malo prijetnejši in hitrejši pregledi. Zato ne more upravičiti tega, da ti ukrepi zelo posegajo v temeljne pravice in svoboščine posameznikov, obdelave iz scenarija 3.2 pa ni mogoče šteti za sorazmerno.

91. EOVP ob upoštevanju teh premislekov v odgovoru na vprašanje 2.3.1 ugotavlja, da kadar se obdelava izvaja za posebni namen pospešitve pretoka potnikov na letališčih, obdelava iz scenarija 3.2:

- **ne more biti združljiva s 25. členom Splošne uredbe o varstvu podatkov,**
- **ne bi bila v skladu s točko f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov**, če bi se upravljavec omejil na ukrepe, opisane v scenariju 3.2, ter
- **ne bi bila v skladu s točko e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov**, ker obdobje hrambe, predvideno v scenariju 3.2, na podlagi informacij, ki so na voljo EOVP, ni dovolj utemeljeno. Da bi se ravnalo v skladu z načelom omejitve hrambe iz točke e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov, bi moral upravljavec dokazati, da se osebni podatki ne hranijo dlje, kot je potrebno za namene, za katere se obdelujejo.

4 SKLEPNE UGOTOVITVE

92. EOVP glede vprašanja 1.1 na podlagi zahtevka za mnenje francoskega nadzornega organa v zvezi z zahtevami iz točke f prvega odstavka 5. člena ter 25. in 32. člena Splošne uredbe o varstvu podatkov ter na podlagi zgornje analize ugotavlja, da:

93. bi se lahko uporaba tehnologije za prepoznavanje obrazov za biometrično avtentikacijo, namenjena posebej za pospešitev pretoka potnikov na letališčih (na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice), načeloma štela za združljivo z načeloma celovitosti in zaupnosti iz točke f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov v primeru arhitekture za hrambo, kadar se vpisana biometrična predloga vsakega potnika hrani lokalno na njegovi osebni napravi in je pod njegovim izključnim nadzorom, če za to veljajo ustrezni zaščitni ukrepi, kot so opisani v točki 46.

94. EOVP glede vprašanja 2.1.1 na podlagi zahtevka za mnenje francoskega nadzornega organa v zvezi z zahtevami iz točk e in f prvega odstavka 5. člena ter 25. in 32. člena Splošne uredbe o varstvu podatkov ter na podlagi zgornje analize ugotavlja, da:

95. bi se lahko uporaba tehnologije za prepoznavanje obrazov za biometrično avtentikacijo, namenjena pospešitvi pretoka potnikov na letališčih (na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice), načeloma štela za združljivo z načelom omejitve hrambe iz točke e prvega odstavka 5. člena, načeloma celovitosti in zaupnosti iz točke f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov v primeru centralizirane arhitekture za hrambo, kadar se vpisana biometrična predloga vsakega potnika v šifrirani obliki hrani v osrednji podatkovni

zbirki na letališču in je pod nadzorom upravljavca letališča, ključ oziroma skrivni podatek pa pozna le posameznik, če za to veljajo ustrezni zaščitni ukrepi, kot so opisani v točki 60.

96. EOVP glede vprašanja 2.2.1 na podlagi zahtevka za mnenje francoskega nadzornega organa v zvezi z zahtevami iz točk e in f prvega odstavka 5. člena ter 25. in 32. členom Splošne uredbe o varstvu podatkov ter na podlagi zgornje analize ugotavlja, da:

97. uporaba tehnologije za prepoznavanje obrazov za biometrično identifikacijo, namenjena pospešitvi pretoka potnikov na letališčih (na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice), v primeru centralizirane arhitekture za hrambo, kadar vpisane biometrične predloge potnikov niso šifrirane s ključem oziroma skrivnim podatkom, ki ga pozna le posamezni potnik, če se take predloge hranijo v podatkovni zbirki na letališču (pod nadzorom upravljavca letališča), ne more biti združljiva s 25. členom Splošne uredbe o varstvu podatkov. Poleg tega taka obdelava ne bi bila v skladu z načeloma celovitosti in zaupnosti iz točke f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov, če bi se upravljavec omejil na ukrepe, kot so opisani v scenariju 3.1.

98. EOVP glede vprašanja 2.3.1 na podlagi zahtevka za mnenje francoskega nadzornega organa v zvezi z zahtevami iz točk e in f prvega odstavka 5. člena ter 25. in 32. člena Splošne uredbe o varstvu podatkov ter na podlagi zgornje analize ugotavlja, da:

99. uporaba tehnologije za prepoznavanje obrazov za biometrično identifikacijo, namenjena pospešitvi pretoka potnikov na letališčih (na varnostnih kontrolnih točkah, pri oddaji prtljage, vkrcanju in dostopu do potniške čakalnice), v primeru centralizirane arhitekture za hrambo, kadar vpisane biometrične predloge potnikov niso šifrirane s ključem oziroma skrivnim podatkom, ki ga pozna le posamezni potnik, če se take predloge hranijo v oblaku (pod nadzorom letalske družbe), ne more biti združljiva s 25. členom Splošne uredbe o varstvu podatkov. Poleg tega taka obdelava ne bi bila v skladu z načeloma celovitosti in zaupnosti iz točke f prvega odstavka 5. člena in 32. členom Splošne uredbe o varstvu podatkov, če bi se upravljavec omejil na ukrepe, kot so opisani v scenariju 3.2. Na podlagi opisa scenarija 3.2 in informacij, ki so na voljo EOVP, obdelava ne bi bila v skladu z načelom omejitve hrambe iz točke e prvega odstavka 5. člena Splošne uredbe o varstvu podatkov.

Za Evropski odbor za varstvo podatkov

predsednica

(Anu Talus)