Mišljenje 11/2024 o upotrebi prepoznavanja lica radi ubrzavanja protoka putnika u zračnim lukama (usklađenost s člankom 5. stavkom 1. točkama (e) i (f), člancima 25. i 32. Opće uredbe o zaštiti podataka (OUZP))

Verzija 1.1

Doneseno 23. svibnja 2024.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Doneseno

Verzija 1.1	28. svibnja 2024.	Gramatički ispravak u sažetku (stranice 3. i 4.) i točkama 77. i 90. Mišljenja
Verzija 1.0	23. svibnja 2024.	Donošenje Mišljenja

Sažetak

Francusko nadzorno tijelo zatražilo je Europski odbor za zaštitu podataka (Odbor, EDPB) da izda mišljenje o upotrebi tehnologije prepoznavanja lica od strane upravitelja zračnih luka i zračnih prijevoznika za biometrijsku autentifikaciju ili identifikaciju putnika radi ubrzanja protoka putnika u zračnim lukama.

Odbor najprije podsjeća da upotreba biometrijskih podataka, a posebno tehnologije prepoznavanja lica, podrazumijeva povećane rizike za prava i slobode ispitanika. To se odnosi na obradu biometrijskih podataka koja je posebno zaštićena na temelju članka 9. OUZP-a. Prije upotrebe takvih tehnologija, čak i ako se smatraju posebno učinkovitima, voditelji obrade trebali bi procijeniti njihov utjecaj na temeljna prava i slobode ispitanika te razmotriti može li se manje nametljivim sredstvima ostvariti zakonita svrha obrade.

Opseg ovog mišljenja, u skladu sa zahtjevom, ograničeno je na usklađenost obrade s **člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a** za **posebnu svrhu ubrzavanja protoka putnika u zračnim lukama** na četiri posebne kontrolne točke, odnosno na zaštitnim kontrolnim točkama, pri predaji prtljage, ukrcaju i prilazu salonu za putnike. Ovo mišljenje ne uključuje potpunu i cjelovitu analizu toga pridržavaju li se relevantni voditelji obrade i, ako postoje, njihovi izvršitelji obrade OUZP-a u svakom pojedinačnom slučaju. Stoga se ovim mišljenjem ne dovodi u pitanje pravna i tehnička analiza svakog pojedinačnog slučaja, koja se temelji na konkretnoj obradi koju je predvidio voditelj obrade i posebnim okolnostima. Osim toga, analiza primjenjive pravne osnove nije obuhvaćena pitanjima upućenima Odboru u zahtjevu te se stoga u ovom mišljenju ne ispituje valjanost privole za takvu obradu, u skladu s člancima 6., 7. i 9. OUZP-a. Osim toga, ovim se mišljenjem ne dovode u pitanje ograničenja uporabe biometrijskih podataka utvrđena pravom države članice.

U ovom mišljenju Odbor ocjenjuje usklađenost obrade s prethodno navedenim odredbama OUZP-a u okviru **četiri specifična scenarija**.

Prvi scenarij uključuje pohranjivanje upisanog biometrijskog predloška kod pojedinca, na primjer, na njegovu osobnom uređaju, nad kojim samo on ima kontrolu kako bi se provela autentifikacija putnika (usporedba 1:1) dok prolazi kroz prethodno navedene kontrolne točke u zračnoj luci.

Odbor zaključuje da bi se moglo smatrati da su odabrane mjere u skladu s načelom nužnosti ako voditelj obrade može dokazati da ne postoje manje nametljiva alternativna rješenja kojima bi se isti cilj mogao postići jednako učinkovito. Osim toga, nametljivost obrade može se kompenzirati aktivnim sudjelovanjem putnika jer se njihov biometrijski predložak pohranjuje samo kod njih, primjerice na njihovu osobnom uređaju, nad kojim samo oni imaju kontrolu, a njihovi se podaci brišu ubrzo nakon dovršetka uspoređivanja. Na temelju toga Odbor zaključuje da se obrada predviđena u prvom scenariju **može smatrati načelno usklađenom s člankom 5. stavkom 1. točkom (f), člancima 25. i 32. OUZP-a** ako se provedu odgovarajuće zaštitne mjere.

Odbor je utvrdio minimalne zaštitne mjere koje bi trebalo provesti za rješenje slično prvom scenariju.

Drugi scenarij uključuje centraliziranu pohranu, unutar zračne luke, upisanog biometrijskog predložaka u šifriranom obliku s ključem/lozinkom, koju posjeduje samo putnik. Time se omogućuje autentifikacija putnika (usporedba 1:1) dok prolaze kroz prethodno navedene zaštitne kontrolne točke u zračnoj luci. Upis vrijedi za određeno razdoblje, koje, na primjer, može trajati do godinu dana nakon posljednjeg leta ili do datuma isteka putovnice.

Odbor zaključuje da bi se moglo smatrati da je obrada u skladu s načelom nužnosti ako voditelj obrade može dokazati da ne postoje manje nametljiva alternativna rješenja kojima bi se isti cilj mogao postići jednako učinkovito. Osim toga, nametljivost obrade može se kompenzirati aktivnim sudjelovanjem putnika jer samo oni imaju kontrolu nad ključem/lozinkom za svoje šifrirane biometrijske podatake. Ako voditelj obrade provodi odgovarajuće zaštitne mjere, sigurnosni rizici povezani s upotrebom centralizirane baze podataka u tom bi se scenariju mogli ublažiti, a negativan učinak na temeljna prava i slobode ispitanika mogao bi se smatrati proporcionalnim očekivanoj koristi. Kad je riječ o načelu ograničenja pohrane, Odboru nisu dostavljene informacije koje bi opravdale dugo razdoblje pohrane. Kako bi se u tom scenariju postigla usklađenost s člankom 5. stavkom 1. točkom (e) OUZP-a, voditelji obrade trebali bi moći opravdati zašto je predviđeno razdoblje pohrane potrebno za određenu svrhu u konkretnim slučajevima. Odbor preporučuje da voditelji obrade predvide najkraće moguće razdoblje pohrane, a putnicima ponude mogućnost da odrede željeno razdoblje pohrane. Na temelju toga Odbor zaključuje da se obrada predviđena u drugom scenariju **može smatrati načelno usklađenom s člankom 5. stavkom 1. točkama (e) i (f), člancima 25. i 32. OUZP-a** ako se provedu odgovarajuće zaštitne mjere.

Odbor je utvrdio minimalne zaštitne mjere koje bi trebalo provesti za rješenje slično drugom scenariju.

Treći scenarij uključuje centraliziranu pohranu unesenog biometrijskog predloška u šifriranom obliku u zračnoj luci pod kontrolom upravitelja zračne luke. To omogućuje identifikaciju putnika (usporedba 1:N) dok prolaze kroz navedene zaštitne kontrolne točke u zračnoj luci. Razdoblje pohrane u ovom scenariju obično je 48 sati, a podaci se brišu nakon što zrakoplov poleti.

S obzirom na to da se osobni i biometrijski podaci pohranjuju u središnjoj bazi podataka ugrožavanje povjerljivost baze podataka može dovesti do pristupa cijelom skupu podataka i omogućiti neovlaštenu ili nezakonitu identifikaciju putnika u drugim okruženjima. Arhitektura centralizirane pohrane pod kontrolom upravitelja zračne luke ujedno dovodi do toga da putnik u većoj mjeri gubi kontrolu nad svojim podacima. Odbor smatra da se rezultat sličan ubrzavanju protoka putnika u zračnim lukama može postići na manje nametljiv način te da je negativan učinak na temeljna prava i slobode ispitanika, koji bi bio posljedica povrede podataka u centraliziranoj bazi biometrijskih podataka, veći od očekivane koristi takve obrade. Stoga obrada ne može zadovoljiti načela nužnosti i proporcionalnosti. Na temelju toga Odbor zaključuje da obrada predviđena u trećem scenariju **ne može biti u skladu s člankom 25. OUZP-a**. Osim toga, takva obrada **ne bi bila u skladu s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a** ako bi se voditelj obrade primjenjivao samo mjere opisane u tom scenariju.

Četvrti scenarij uključuje centraliziranu pohranu upisanog biometrijskog predloška u šifriranom obliku u oblaku pod kontrolom zračnog prijevoznika ili njegova pružatelja usluga u oblaku. To omogućuje identifikaciju putnika (usporedba 1:N) dok prolaze kroz prethodno navedene zaštitne kontrolne točke u zračnoj luci. Razdoblje pohrane u tom scenariju može trajati sve dok putnik ima račun kod zračnog prijevoznika.

Budući da se osobni i biometrijski podaci pohranjuju u središnjoj bazi podataka u oblaku, pristup takvim podacima moglo bi imati više subjekata, uključujući moguće pružatelje s poslovnim nastanom izvan EGP-a. Podaci putnika dešifriraju se kad se koriste, a ključevi su pod kontrolom zračnog prijevoznika ili njegovih izvršitelj obrade, što bi moglo povećati površinu sigurnosne izloženosti. Takva centralizirana arhitektura pohrane ujedno dovodi do toga da putnici u većoj mjeri gube kontrolu nad svojim podacima. Podaci bi se mogli pohranjivati i tijekom duljeg razdoblja, što ih izlaže većim rizicima od povrede sigurnosti i čini se da nadilazi ono što je strogo nužno i proporcionalno za potrebe obrade, osim ako se poduzmu daljnje očite mjere za ublažavanje rizika za pojedince.

Odbor smatra da se rezultat sličan ubrzavanju protoka putnika u zračnim lukama može postići na manje nametljiv način te da je negativan učinak na temeljna prava i slobode ispitanika, koji bi mogao biti posljedica povrede podataka u središnjoj bazi biometrijskih podataka, veći od očekivane koristi takve obrade. Stoga obrada ne može zadovoljiti načela nužnosti i proporcionalnosti. Na temelju toga Odbor zaključuje da obrada predviđena u četvrtom scenariju **ne može biti u skladu s člankom 25. OUZP-a**. Također, takva obrada **ne bi bila u skladu s člankom 5. stavkom 1. točkom (e) OUZP-a** na temelju informacija dostupnih Odboru **niti u skladu s člankom 5. stavkom 1. točkom (f) i člankom 32. te uredbe** ako bi voditelj obrade primjenjivao samo mjere opisane u tom scenariju.

Sadržaj

uzimajući u obzir članak 63. i članak 64. stavak 2. Uredbe 2016/679/EU Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „**OUZP**"),

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članke 10. i 22. Poslovnika Europskog odbora za zaštitu podataka (dalje u tekstu „**Odbor**" ili „**EDPB**") (dalje u tekstu „**Poslovnik EDPB-a**"),

budući da:

(1) Glavna uloga Odbora je osigurati dosljednu primjenu OUZP-a u cijelom Europskom gospodarskom prostoru (dalje u tekstu „**EPG**"). Člankom 64. stavkom 2. OUZP-a propisano je da svako nadzorno tijelo, predsjednik Odbora ili Komisija mogu zatražiti da svaki predmet opće primjene ili s učincima u više od jedne države članice EPG-a ispita Odbor kako bi dao mišljenje.

(2) Mišljenje Odbora donosi se u skladu s člankom 64. stavkom 3. OUZP-a u vezi s člankom 10. stavkom 2. Poslovnika Odbora u roku od osam tjedana nakon što predsjednik i nadležno nadzorno tijelo utvrde da su dokumenti potpuni. Odlukom predsjednika to se razdoblje može produljiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta,

DONIO JE SLJEDEĆE MIŠLJENJE:

1. UVOD

1.1. Sažetak činjenica

1. Francusko nadzorno tijelo zatražilo je 16. veljače 2024. od Odbora da izda mišljenje o usklađenosti s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a upotrebe tehnologije prepoznavanja lica od strane upravitelja zračnih luka i zračnih prijevoznika za biometrijsku autentifikaciju ili identifikaciju putnika[2], kako bi se ubrzao protok putnika, na zaštitnim kontrolnim točkama u zračnoj luci luke[3], pri predaji prtljage, ukrcaju i pristupu salonu za putnike (isključujući graničnu kontrolu i kontrole koje provode bescarinske trgovine) (dalje u tekstu „**Zahtjev**"). Francusko nadzorno tijelo priložilo je svojem zahtjevu opis uobičajenih slučajeva upotrebe (Prilog I.).

[1] Upućivanja na „države članice" u ovom mišljenju treba tumačiti kao upućivanja na „države članice EGP-a". Upućivanja na „Uniju" u ovom mišljenju treba tumačiti kao upućivanja na „EGP".
[2] U kontekstu ovog mišljenja „**putnik**" znači ispitanik čiji se osobni podaci obrađuju u posebnu svrhu opisanu u ovom mišljenju. U daljnjem tekstu ovog mišljenja, pojmovi „putnik" i „pojedinac" međusobno su zamjenjiva.
[3] Za potrebe ovog mišljenja, „**točke za zaštitnu provjeru u zračnoj luci**" odnosi se na zaštitne provjere koje se provode pod odgovornošću upravitelja zračne luke i kojima se putnici moraju podvrgnuti kako bi ušli iz dvorane za odlaske u prostor ili izlaz za ukrcaj.

2. Francusko nadzorno tijelo u svojem zahtjevu primjećuje da različite države članice trenutačno ispituju različite modele zbog čega može doći do razlika u tumačenjima među nadzornim tijelima i rizika od različitih učinaka na temeljna prava i slobode ispitanika u EU-u[4].

3. Odbor smatra da je za odgovor na Zahtjev potrebno odgovoriti na sljedeća pitanja:

4. **Prvo pitanje:**

1.1. Može li upotreba tehnologije prepoznavanja lica za autentifikaciju na temelju biometrijskih podataka **u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama** (zaštitne kontrolne točke, predaja prtljage, ukrcaj i pristup salonu za putnike) biti usklađena s **člankom 5. stavkom 1. točkom (f), člancima 25. i 32. OUZP-a,** kad je riječ o arhitekturi za pohranu podataka, u kojoj je biometrijski predložak svakog putnika pohranjen **samo kod njega**, npr. lokalno na njegovu osobnom uređaju nad kojim samo on ima kontrolu?

1.2. Ako bi se takva obrada smatrala usklađenom s prethodno navedenim odredbama, koje bi minimalne odgovarajuće zaštitne mjere bile potrebne s obzirom na članke 25. i 32. OUZP-a?

Drugo pitanje:

2.1. Može li upotreba tehnologije prepoznavanja lica za autentifikaciju ili identifikaciju na temelju biometrijskih podataka **u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama** (zaštitne kontrolne točke, predaja prtljage, ukrcaj i pristup salonu za putnike) biti usklađena s **člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a** kad je riječ o arhitekturi za **centraliziranu** pohranu podataka, u kojoj je biometrijski predložak svakog putnika pohranjen u središnjoj bazi podataka:

2.1.1. U središnjoj bazi podataka u zračnoj luci, pod kontrolom upravitelja zračne luke, u šifriranom obliku, s ključem/lozinkom koju posjeduje samo pojedinac (na primjer na njegovu mobilnom telefonu), radi autentifikacije?

2.1.2. Ako bi se takva obrada smatrala usklađenom, koje bi minimalne odgovarajuće zaštitne mjere bile potrebne s obzirom na članke 25. i 32. OUZP-a?

2.2.1. U središnjoj bazi podataka unutar zračne luke, pod kontrolom upravitelja zračne luke, u šifriranom obliku, s ključevima koje čuva upravitelj zračne luke, radi identifikacije?

2.2.2. Ako bi se takva obrada smatrala usklađenom, koje bi minimalne odgovarajuće zaštitne mjere bile potrebne s obzirom na članke 25. i 32. OUZP-a?

2.3.1. U oblaku, pod kontrolom zračnog prijevoznika ili njegova pružatelja usluga (izvršitelja obrade), u šifriranom obliku, s ključevima koje čuva zračni prijevoznik ili njegov pružatelj usluga, radi identifikacije?

2.3.2. Ako bi se takva obrada smatrala usklađenom, koje bi minimalne odgovarajuće zaštitne mjere bile potrebne s obzirom na članke 25. i 32. OUZP-a?

[4] Zahtjev, str 1.

5. Nakon što je francusko nadzorno tijelo 16. veljače 2024. utvrdilo da je spis potpun, a predsjednik Odbora 23. veljače 2024. je to potvrdio, Tajništvo je spis proslijedilo 23. veljače 2024. U skladu s člankom 64. stavkom 3. OUZP-a povezano s člankom 10. stavkom 2. Poslovnika EDPB-a predsjednik Odbora odlučio je produljiti zadani rok od osam tjedana za još šest tjedana zbog složenosti predmeta.

1.2. Dopuštenost zahtjeva za mišljenje na temelju članka 64. stavka 2. OUZP-a

6. Člankom 64. stavkom 2. OUZP-a propisano je da svako nadzorno tijelo može zatražiti da svaki predmet opće primjene ili s učincima u više od jedne države članice pregleda Odbor kako bi on dao mišljenje.

7. Odbor smatra da se zahtjev koji je uputilo francusko nadzorno tijelo o usklađenosti upotrebe tehnologije prepoznavanja lica za biometrijsku autentifikaciju ili identifikaciju u svrhu ubrzavanja protoka putnika u zračnim lukama odnosi na pitanja „s učincima u više od jedne države članice", jer, kako je objašnjeno u zahtjevu[5], trenutačno je u tijeku nekoliko projekata u zračnim lukama država članica te se procjenjuje da će se takva upotreba povećati u nadolazećim godinama. Modeli koje trenutačno ispituju različite zračne luke i zračni prijevoznici znatno se razlikuju od jedne države članice do druge zbog čega može doći do rizika da bi, sa stajališta zaštite podataka, to moglo proizvesti različite učinke u više država članica.

8. Osim toga, Odbor smatra da Zahtjev koji je uputilo francusko nadzorno tijelo ima važne posljedice za primjenu načela utvrđenih u članku 5. stavku 1. točkama (e) i (f) OUZP-a te zahtjeva koji se primjenjuju na voditelje obrade na temelju članka 25. te uredbe, kao i zahtjeva koji se primjenjuju na voditelje i izvršitelje obrade na temelju članka 32. iste uredbe. Stoga se ovaj Zahtjev odnosi na „pitanje opće primjene" u smislu članka 64. stavka 2. OUZP-a jer se odnosi na dosljedno tumačenje načela ograničenja pohrane (članak 5. stavak 1. točka (e) OUZP-a) te cjelovitosti i povjerljivosti (članak 5. stavak 1. točka (f) OUZP-a) i pojmova tehničke i integrirane zaštite podataka (članak 25. OUZP-a) i sigurnosti podataka (članak 32. OUZP-a) kako bi se, među ostalim, osigurala dosljedna primjena tih odredaba u EGP-u.

9. Moguća različita stajališta u državama članicama o tumačenju članka 5. stavka 1. točaka (e) i (f) te članaka 25. i 32. OUZP-a povećala bi rizik da upravitelji zračnih luka i zračni prijevoznici razvijaju projekte prepoznavanja lica na nedosljedan način. Budući da je francusko nadzorno tijelo pokazalo jasnu potrebu za dosljednim tumačenjem tih odredaba u pogledu tehnologije prepoznavanja lica za biometrijsku autentifikaciju ili identifikaciju putnika kako bi se ubrzao protok putnika u zračnim lukama,[6] Odbor smatra da je zahtjev obrazložen u skladu s člankom 10. stavkom 3. Poslovnika EDPB-a.

10. U skladu s člankom 64. stavkom 3. OUZP-a EDPB ne daje mišljenje ako je već dao mišljenje o istoj stvari[7]. EDPB dosad još nije odgovorio na pitanja koja proizlaze iz Zahtjeva. Iako Smjernice EDPB-a 3/2019 o videouređajima[8] već sadržavaju neke korisne elemente o sigurnosnim mjerama koje bi se trebale primjenjivati na obradu biometrijskih podataka, ne obuhvaćaju sve aspekte pitanja postavljenih u Zahtjevu. Nadalje, dostupne smjernice EDPB-a, uključujući Smjernice 3/2019 o

[5] Zahtjev, str 3.
[6] Zahtjev, str. 1.–3.
[7] Članak 64. stavak 3. OUZP-a i članak 10. stavak 4. Poslovnika EDPB-a.
[8] Smjernice EDPB-a 3/2019 o obradi osobnih podataka putem videouređaja, verzija 2.0, donesene 29. siječnja 2020. (dalje u tekstu „**Smjernice EDPB-a 3/2019 o videouređajima**").

videouređajima, ne sadržavaju posebne smjernice o mogućim elementima koje treba provjeriti u vezi s centraliziranom ili decentraliziranom pohranom biometrijskih podataka za identifikaciju ili autentifikaciju putnika radi ubrzavanja protoka putnika u zračnim lukama, niti o usklađenosti takve obrade s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a.

11. Zbog toga Odbor smatra da je zahtjev dopušten, a pitanja koja iz njega proizlaze trebalo bi analizirati u Mišljenju („Mišljenje"), donesenom u skladu s člankom 64. stavkom 2. OUZP-a.

2. PODRUČJE PRIMJENE I KONTEKST MIŠLJENJA

2.1. Područje primjene mišljenja

12. Ovo se mišljenje odnosi samo na usklađenost upotrebe tehnologije prepoznavanja lica za biometrijsku autentifikaciju ili identifikaciju putnika od strane upravitelja zračnih luka i zračnih prijevoznika, **u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama**, odnosno na zaštitnim kontrolnim točkama, pri predaji prtljage, ukrcaju i prilazu salonu za putnike s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a, kako je opisano u Zahtjevu.

13. Što se tiče **područja primjene ovog mišljenja**, Odbor pojašnjava sljedeće:

1) Obrada osobnih podataka u okviru graničnih kontrola i kontrola koje provode bescarinske trgovine nisu obuhvaćene ovim mišljenjem jer ih provode voditelji obrade koji nisu upravitelji zračnih luka i zračni prijevoznici.

2) Upotreba tehnologije prepoznavanja lica, čak i ako se temelji na scenarijima opisanim u odjeljku 3.2. u nastavku, u bilo koje druge svrhe (kao što je izvršavanje zakonodavstva) ili ih provode druge strane, čak i ako se upotrebljava u slične svrhe, nije obuhvaćena područjem primjene ovog mišljenja.

3) Ovo se mišljenje odnosi samo na obradu osobnih podataka putnika i ne obuhvaća druge vrste ispitanika, kao što su osoblje upravitelja zračnih luka ili zračnih prijevoznika.

4) U ovom mišljenju razmatra se zahtjev koji je podnijelo francusko nadzorno tijelo o usklađenosti arhitekture pohrane biometrijskih predložaka putnika s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a. U tom pogledu ovo mišljenje ne uključuje potpunu i cjelovitu analizu toga pridržavaju li se, ako je to potrebno, relevantni voditelji obrade i njihovi izvršitelji obrade OUZP-a. To je posebno važno s obzirom na to da te tehnologije podrazumijevaju povećane rizike povezane s obradom posebnih kategorija podataka u skladu s člankom 9. Opće uredbe o zaštiti podataka. Stoga se ovim mišljenjem ne dovodi u pitanje procjena o drugim odredbama OUZP-a kad je riječ o upotrebi tehnologija prepoznavanja lica, među ostalim u određenom sektoru na koji se Zahtjev odnosi, ni pravna i tehnička analiza u pojedinačnom slučaju, koja se temelji na konkretnoj obradi koju je predvidio voditelj obrade i posebnim okolnostima.

5) U ovom se mišljenju ne ispituje obrada osobnih podataka djece i ne dovode se u pitanje posebni zahtjevi koji se u tom pogledu primjenjuju.

6) Ovim se mišljenjem ne dovode u pitanje pravni zahtjevi i daljnja ograničenja uporabe biometrijskih podataka koji proizlaze iz nacionalnih zakona država članica[9].

7) Nijedan zaključak u ovom mišljenju ne dovodi u pitanje daljnji tehnološki razvoj.

8) U ovom se mišljenju ispituju četiri scenarija čije su posebne značajke opisane u odjeljku 3.2. Ne odnosi se na druge scenarije, čak i ako se obrada provodi u iste svrhe.

14. Francusko nadzorno tijelo u svojem je Zahtjevu navelo da bi se obrada biometrijskih podataka putnika u svrhu ubrzanja protoka putnika u zračnim lukama temeljila na pretpostavci da pojedinci pristaju na takvu obradu, što bi mogla biti pravna osnova na temelju OUZP-a[10]. **Međutim, analiza primjenjive pravne osnove nije obuhvaćena pitanjima upućenim EDPB-u u Zahtjevu te se stoga u ovom mišljenju ne ispituje valjanost privole za takvu obradu, u skladu s člancima 6., 7. i 9. OUZP-a.**

15. Međutim, EDPB općenito napominje da bi relevantni voditelji obrade, ako bi se oslanjali na tu pravnu osnovu, morali dobiti valjanu izričitu privolu[11] od pojedinaca koji su voljni koristiti takve usluge. Takva izričita privola trebala bi biti dobrovoljna, konkretna i informirana[12], a hoće li ti uvjeti biti ispunjeni, analizirat će se u svakom pojedinačnom slučaju. To, među ostalim, znači sljedeće:

1) Pojedinci bi trebali moći jednostavno povući takvu privolu u bilo kojem trenutku i bez ikakvih posljedica[13].

2) Kako bi privola bila dobrovoljna, takva upotreba biometrijskih tehnologija može se odvijati samo na dobrovoljnoj osnovi jer bi pojedinci trebali moći slobodno odabrati hoće li se koristiti tim uslugama i to bez ikakvih posljedica (kao što su znatno dulja kašnjenja za putnike koji ne daju privolu[14]), poticaja, dodatnih troškova ili dobivanja dodatnih pogodnosti zauzvrat[15].

3) Izričitu privolu trebalo bi tražiti i od pojedinaca čiji se biometrijski podaci obrađuju, čak i ako nisu upisani radi identifikacije ili autentifikacije takvim sredstvima. Drugim riječima, važno je da se lica pojedinaca koji nisu izričito pristali na prepoznavanje lica u predviđenu svrhu ne skeniraju kamerama. To se može postići, na primjer, tako da se odrede posebne trake za prepoznavanje lica te da se one odvoje odgovarajućim

[9] Na primjer, člankom 9. stavkom 4. OUZP-a predviđa se da države članice mogu zadržati ili uvesti dodatne uvjete, uključujući ograničenja, u pogledu obrade biometrijskih podataka.
[10] Zahtjev, Prilog I.
[11] U skladu s člankom 4. stavkom 14., člankom 9. stavkom 1. i člankom 9. stavkom 2. točkom (a) OUZP-a, zabranjena je obrada biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, osim ako je ispitanik dao izričitu privolu za obradu tih osobnih podataka za jednu ili više utvrđenih svrha, osim ako je pravom Unije ili pravom države članice predviđeno da ispitanik ne može ukinuti zabranu iz članka 9. stavka 1. te uredbe. Vidjeti i uvodne izjave 51., 52. i 53. OUZP-a.
[12] Članak 4. stavak 11. i članak 7. OUZP-a
[13] Članak 7. stavak 4. i uvodna izjava 50. OUZP-a.
[14] Na primjer, to može uključivati razmatranja kao što je osmišljavanje sustava kako bi se izbjeglo stvaranje društvenog pritiska na putnike koji ne žele dati privolu tako da se izbjegne to da njihov izbor negativno utječe na druge putnike.
[15] Smjernice EDPB-a 05/2020 o privoli na temelju Uredbe 2016/679, verzija 1.1., donesene 4. svibnja 2020. (dalje u tekstu „**Smjernice Europskog odbora za zaštitu podataka 5/2020 o privoli**"), točke 46. i 48.

oznakama i fizički od kontrolnih tokova koji nisu za biometrijske svrhe kako bi se mogle jasno razlikovati od ostalih traka.

4) Ne dovodeći u pitanje bi li privola bila primjenjiva pravna osnova za takvu obradu, načela obrade iz članka 5. OUZP-a koja se odnose na nužnost i proporcionalnost i dalje se primjenjuju čak i ako su pojedinci dali izričitu privolu za upotrebu svojih biometrijskih podataka[16].

16. U Zahtjevu se navodi[17] da bi upravitelji zračnih luka djelovali kao voditelji obrade za obradu na zaštitnim kontrolnim točaka u zračnoj luci, dok bi zračni prijevoznici djelovali kao voditelji obrade za obradu pri predaji prtljage, ukrcaju i pristupu salon za putnike. Odbor stoga napominje da bi u obradu opisanu u Zahtjevu mogli biti uključeni različiti dionici i nije procijenio primjenu uloga (zajedničkog) voditelja obrade i/ili izvršitelja obrade u scenarijima opisanim u nastavku u odjeljku 3.2. ovog mišljenja. U svakom slučaju potrebno je utvrditi uključene dionike i dodijeliti im jasne odgovornosti kako bi se ispunili zahtjevi OUZP-a[18].

17. Osim toga, Odbor napominje da trenutačno ne postoji ujednačena pravna obveza u EU-u za upravitelje zračnih luka i zračne prijevoznike da identificiraju putnike i provjeravaju podudara li se ime na karti za ukrcaj u zrakoplov putnika s imenom na njihovoj identifikacijskoj ispravi na svim prethodno navedenim zaštitnim kontrolnim točkama[19]. Stoga svi takvi zahtjevi podliježu nacionalnim zakonima koji se mogu razlikovati od jedne države članice do druge. U nekim državama članicama takva provjera može biti potrebna za neke zaštitne kontrolne točke (npr. predaju prtljage ili ukrcaj), dok u drugima takve provjere danas nisu potrebne[20]. Postojanje zakonskih obveza provjere identiteta putnika izravno utječe na prakse različitih zračnih luka.

18. Iz toga proizlazi da u tim situacijama, **ako nije potrebna provjera identiteta putnika službenom identifikacijskom ispravom, ne bi se trebala provoditi provjera s pomoću biometrijskih podataka jer bi to dovelo do prekomjerne obrade podataka budući da podrazumijeva obradu dodatnih podataka u usporedbi s trenutačnom situacijom i nadilazilo bi ono što je potrebno za relevantnu svrhu, čime bi se prekršilo načelo smanjenja količine podataka utvrđeno u članku 5. stavku 1. točki (c) OUZP-a.** Takvo razmatranje treba uzeti u obzir pri ispitivanju svih scenarija opisanih u odjeljku 3.2. ovog mišljenja.

2.2. Ključni pojmovi

[16] Idem, točka 5.
[17] Zahtjev, Prilog I.
[18] U skladu s člankom 4. stavcima 7. i 8., člankom 5. stavkom 2., člancima 24., 26., 28. i 29. OUZP-a. Vidjeti i Smjernice 07/2020 EDPB-a o pojmovima voditelja i izvršitelja obrade u Općoj uredbi o zaštiti podataka, verzija 2.1, donesene 7. srpnja 2021.
[19] Relevantna uredba na razini EU-a je Provedbena uredba Komisije (EU) 2015/1998 od 5. studenoga 2015. o utvrđivanju detaljnih mjera za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa. Međutim, ta se uredba ne odnosi se na provjere službenih identifikacijskih isprava na kontrolnim točkama u zračnim lukama, a države članice imaju diskrecijsko pravo regulirati to pitanje na nacionalnoj razini.
[20] To znači da se trenutačno uopće ne provodi provjera ili se provjerava samo postojanje kartu za ukrcaj u zrakoplov. Na primjer, na temelju Protokola o izuzeću državljana Danske, Finske, Norveške i Švedske od obveze posjedovanja putovnice ili boravišne dozvole dok borave u skandinavskoj zemlji koja nije njihova matična zemlja od 22. svibnja 1954., od 1. srpnja 1954. državljani Norveške, Danske, Finske i Švedske izuzeti su od obveze posjedovanja putovnice ili druge putne isprave kad putuju iz jedne u drugu od tih zemalja.

19. Kako bi se smatrali biometrijskim podacima u skladu s člankom 4. stavkom 14. OUZP-a[21], obrada neobrađenih podataka, kao što su fizička i fiziološka obilježja ili obilježja ponašanja pojedinca, trebala bi podrazumijevati mjerenje tih obilježja jer su biometrijski podaci rezultat takvih mjerenja[22].

20. Upotrebom slike lica pojedinca (fotografije ili videozapisa) koja se naziva biometrijski „**uzorak**", moguće je izdvojiti digitalni prikaz različitih obilježja takvog lica (to se naziva „**predložak**")[23]. Osim toga, Odbor podsjeća da je „biometrijski predložak digitalni prikaz jedinstvenih značajki izdvojenih iz biometrijskog uzorka, koje se mogu pohraniti u biometrijskoj bazi podataka"[24] kojima se omogućuje ili potvrđuje jedinstvena identifikacija fizičke osobe. Nadalje, „[t]aj biometrijski predložak trebao bi biti jedinstven i specifičan za svaku osobu te je u načelu stalan tijekom vremena"[25]. U postupku usporedbe čiji je cilj identifikacija ili autentifikacija pojedinca prepoznavanjem lica, ulazni biometrijski predložak obično se uspoređuje s pohranjenim objektima kako bi se provjerila podudarnost ili pronašlo podudaranje u bazi podataka[26].

21. Tehnologija prepoznavanja lica može ispunjavati dvije različite funkcije, odnosno autentifikaciju[27] i identifikaciju[28]. Iako su obje funkcije različite, obje se temelje na obradi biometrijskih podataka povezanih s identificiranom fizičkom osobom ili fizičkom osobom koju se može identificirati[29] te stoga predstavljaju obradu posebnih kategorija osobnih podataka na temelju članka 9. OUZP-a[30].

22. Konkretnije:

> Cilj je **autentifikacije** potvrditi biometrijsku tvrdnju usporedbom. To se ujedno naziva provjera 1 prema 1.

---

[21] Vidjeti uvodne izjave 51., 52. i 53. OUZP-a.

[22] Smjernice EDPB-a 3/2019 o videouređajima, točka 74.

[23] Smjernice EDPB-a 05/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva, verzija 2.0, donesene 26. travnja 2023. (dalje u tekstu: **Smjernice EDPB-a 5/2022 o prepoznavanju lica u području izvršavanja zakonodavstva**), točke 7. i 8.

[24] Idem, točka 9.

[25] Idem.

[26] Smjernice EDPB-a 5/2022 o prepoznavanju lica u provedbi zakona, točke 10. i 11.; vidjeti i međunarodnu normu ISO/IEC 2382-37, 2022-03, dostupno na: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [posljednji pristup 23. svibnja 2024.] (dalje u tekstu „**ISO/IEC 2382-37**")

[27] Odbor napominje da se u predstojećoj Uredbi Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) (još nije objavljeno u Službenom listu) u članku 3. točki 36. „biometrijska provjera" definira i kao automatizirana provjera usporedbom dvaju uzoraka, uključujući autentifikaciju, kojom se identitet fizičkih osoba provjerava usporedbom njihovih biometrijskih podataka s prethodno dostavljenim biometrijskim podacima" (vidjeti Zakonodavnu rezoluciju Europskog parlamenta od 13. ožujka 2024. o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije (COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Idem, u članku 3. stavku 35. Akta o umjetnoj inteligenciji „biometrijska identifikacija" definirana je kao „automatizirano prepoznavanje fizičkih, fizioloških i bihevioralnih obilježja ljudi u svrhu utvrđivanja identiteta pojedinca usporedbom njegovih biometrijskih podataka s biometrijskim podacima pojedinaca pohranjenima u referentnoj bazi podataka".

[29] ISO/IEC 2382-37.

[30] Članak 4. stavak 14. OUZP-a i Smjernice EDPB-a 5/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva, točka 12.

Cilj je **identifikacije** pretraživanje baze podataka s biometrijskim podacima kako bi se vratile identifikacijske oznake koje se mogu pripisati jednom pojedincu. To se također naziva identifikacija 1 prema mnogima.

23. U oba slučaja (tj. identifikacija i autentifikacija) tehnike prepoznavanja lica temelje se na procijenjenom podudaranju predložaka, tj. onog koji se uspoređuje i početne vrijednosti. S ove točke gledišta, one su probabilističke, odnosno ako se usporedbom utvrdi veća ili manja vjerojatnost da je osoba doista ona koju treba autentificirati ili identificirati te ako ta vjerojatnost prelazi određeni prag u sustavu, koji je definirao korisnik ili programer sustava, sustav će pretpostaviti da postoji podudaranje koje treba identificirati ili potvrditi[31].

[31] Smjernice EDPB-a 5/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva, točka 11. Vidjeti i ISO/IEC 2382-37.

3. O OSNOVANOSTI ZAHTJEVA

3.1. Općenita opažanja

24. U ovom se odjeljku analiziraju pitanja iznesena u točki 4. U tom kontekstu Odbor će za prvo pitanje analizirati usklađenost s člankom 5. stavkom 1. točkom (f) i člancima 25. i 32. Opće uredbe o zaštiti podataka, a za drugo pitanje usklađenost s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. Opće uredbe o zaštiti podataka.

25. U tu će svrhu Odbor analizirati četiri različita scenarija[32], čije su posebne značajke opisana u nastavku u odjeljku 3.2.

26. Odbor najprije podsjeća da upotreba biometrijskih podataka, a posebno tehnologije prepoznavanja lica, podrazumijeva povećane rizike za prava i slobode ispitanika. Kao prvo, predmetna obrada odnosi se na biometrijske podatke koji su posebno zaštićeni na temelju članka 9. Opće uredbe o zaštiti podataka. Konkretno, biometrijski podaci nepovratno mijenjaju odnos između tijela i identiteta jer čine obilježja ljudskog tijela „strojno čitljivima" i podložnima daljnjoj uporabi[33]. Nadalje, upotreba tehnologije prepoznavanja lica može dovesti do rizika povezanih s lažno negativnim rezultatima, pristranosti i diskriminacijom[34], a mogućnost zlouporabe biometrijskih podataka mogla bi imati ozbiljne posljedice za pojedince kao što su prijevara povezana s identitetom ili lažno predstavljanje[35]. Treba napomenuti i da bi, kad se prepoznavanje lica provodi na daljinu i bez aktivnog sudjelovanja ispitanika, pojedinci mogli biti još manje svjesni takve obrade i povezanih rizika. Naposljetku, važno je naglasiti da se obilježja na kojima se temelje biometrijski podaci općenito mogu smatrati trajnima i da bi ih trebalo smatrati neopozivima, posebno u kontekstu prepoznavanja lica[36].

27. Stoga bi, uzimajući u obzir prethodno navedeno, prije upotrebe takvih tehnologija, čak i ako smatraju posebno učinkovitima, voditelji obrade trebali bi procijeniti učinak na temeljna prava i slobode ispitanika te razmotriti mogu li se manje nametljivim sredstvima ostvariti njihova legitimna svrha obrade[37].

---

[32] Četiri scenarija koja je Odbor analizirao temelje se na slučajevima upotrebe navedenima u Prilogu I. zahtjeva. Francusko nadzorno tijelo pojasnilo je da su slučajevi upotrebe navedeni u Prilogu I. Zahtjeva primjeri provedbe koji pripadaju scenariju i koriste se u ilustrativne svrhe.

[33] Mišljenje 3/2012 Radne skupine iz članka 29. o razvoju biometrijskih tehnologija doneseno 27. travnja 2012., RD193 (dalje u tekstu „**Mišljenje 3/2012 Radne skupine iz članka 29. o biometrijskim tehnologijama**"), str. 4. Treba napomenuti da se u ovom mišljenju upućuje na Direktivu 95/46/EZ od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka („Direktiva o zaštiti podataka"). Općom uredbom o zaštiti podataka prošireno je područje primjene posebnih kategorija podataka te se, za razliku od Direktive o zaštiti podataka, predviđa da su biometrijski podaci posebne kategorije podataka (članak 9. Opće uredbe o zaštiti podataka).

[34] Smjernice o prepoznavanju lica, Savjetodavni odbor Konvencije Vijeća Europe za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka, lipanj 2021., str. 15. i Smjernice EDPB-a 5/2022 o prepoznavanju lica u području izvršavanja zakonodavstva, točka 27.

[35] Mišljenje Radne skupine iz članka 29 WP 3/2012 o biometrijskim tehnologijama, str. 29.

[36] Smjernice EDPB-a 5/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva, točka 104.

[37] Uvodna izjava 39. OUZP-a; vidjeti i Smjernice EDPB-a 3/2019 o videouređajima, točka 73.

28. Odbor podsjeća i na to da pravo na zaštitu osobnih podataka nije apsolutno pravo i da bi trebalo uspostaviti ravnotežu između njega i drugih temeljnih prava zaštićenih Poveljom u skladu s načelom proporcionalnosti[38].

29. U članku 25. stavku 1. OUZP-a upućuje se na „načela zaštite podataka" navedena u članku 5. te uredbe[39] i zahtijeva njihovu „učinkovitu" primjenu primjenom tehničke zaštite[40]. To izričito uključuje načelo smanjenja količine podataka na temelju članka 5. stavka 1. točke (c) OUZP-a,[41] kojim se zahtijeva da osobni podaci budu „primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju", čime se konkretizira načelo proporcionalnosti[42]. Osim toga, u članku 25. stavku 2. OUZP-a navodi se obveza „smanjenja količine podataka integriranim načinom" tako što se navodi da se ona primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost[43].

30. Međutim, člankom 25. OUZP-a od voditelja obrade ne zahtijeva se provedba posebnih tehničkih i organizacijskih mjera, već se zahtijeva da odabrane mjere i zaštitne mjere budu specifične za kontekst i rizike za prava i slobode ispitanika koje predstavlja obrada[44]. Slično tome, člankom 32. OUZP-a od voditelja i izvršitelja obrade zahtijeva se da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik za prava i slobode pojedinaca.

31. Važno je napomenuti da, čak i ako putnici izričito pristanu na upotrebu svojih biometrijskih podataka kako bi se ubrzao protok putnika u zračnim lukama, i dalje se primjenjuju načela obrade utvrđena u OUZP-u koja se odnose na nužnost i proporcionalnost te ih je potrebno poštovati[45].

32. Kad je riječ o **načelu nužnosti**, Odbor će razmotriti je li predložena obrada nužna za ostvarivanje željenog cilja i može li se isti cilj jednako učinkovito postići drugim sredstvima kojima se manje zadire

---

[38] Uvodna izjava 4. OUZP-a; S tim u vezi, vidjeti i presudu Suda od 22. lipnja 2021., predmet *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (dalje u tekstu „predmet C-439/19 *Latvijas Republikas Saeima*"), točke 98., 110. i 113. Osim toga, načelo proporcionalnosti, kao opće načelo prava Unije, zahtijeva da su mjere koje se provode aktima Unije prikladne za postizanje željenog cilja i da ne prelaze ono što je nužno za njegovo postizanje (vidjeti presudu Suda od 9. studenoga 2010., predmet *Volker i Markus Schecke i Eifert*, C-92/09 i C-93/09, ECLI:EU:C:2010:662 (dalje u tekstu „predmet C-92/09 i C-93/09 *Volker i Schecke*"), točka 74. i navedena sudska praksa).

[39] Smjernice Europskog odbora za zaštitu podataka 4/2019 o članku 25. Tehnička i integrirana zaštita podataka, verzija 2.0, donesene 20. listopada 2020. (dalje u tekstu „**Smjernice Europskog odbora za zaštitu podataka 4/2019 o tehničkoj i integriranoj zaštiti podataka**"), točka 11.

[40] U članku 25. stavku 1. OUZP-a navodi se sljedeće: „Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika." Vidjeti i Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., točka 13.

[41] U skladu s time, u uvodnoj izjavi 39. Opće uredbe o zaštiti podataka navodi se da bi se osobni podaci trebali obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima.

[42] Predmet C-439/19 *Latvijas Republikas Saeima*, točka 98.; Presuda Suda od 11. prosinca 2019., predmet *Asociația de Proprietari blok M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (dalje u tekstu „predmet C-708/18 *M5A-ScaraA*"), točka 48.

[43] Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., točka 48.

[44] Smjernice 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., str. 14.

[45] Smjernice EDPB-a 5/2020 o privoli na temelju Uredbe 2016/679, točka 5.

u temeljna prava i slobode ispitanika[46]. Kad je riječ o **načelu proporcionalnosti**, Odbor će procijeniti je li negativan učinak na temeljna prava i slobode ispitanika proporcionalan određenoj očekivanoj koristi. Ako je korist relativno mala, takav učinak možda neće biti proporcionalan[47].

33. U svakom slučaju, čak i ako Odbor smatra da bi jedan od scenarija analiziranih u nastavku mogao ispuniti zahtjeve iz članka 5. stavka 1. točaka (e) i (f), članaka 25. i 32. OUZP-a, voditelj obrade to mora činjenično dokazati. Takvo dokazivanje trebalo bi uključivati razmatranje alternativnih scenarija.

3.2. O usklađenosti s člankom 5. stavkom 1. točkama (e) i (f), člancima 25. i 32. OUZP-a

3.2.1. Scenarij 1.: pohrana upisanog biometrijskog predloška samo kod pojedinca radi autentifikacije

34. U ovom se odjeljku ispituje usklađenost pohranjivanja biometrijskog predloška putnika samo kod pojedinca, na primjer na njegovu osobnom uređaju[48], nad kojim samo on ima kontrolu[49], radi autentifikacije[50] s člankom 5. stavkom 1. točkom (f) i člancima 25. i 32. Opće uredbe o zaštiti podataka (dalje u tekstu „**prvi scenarij**"). U ovom se odjeljku ispituju i odgovarajuće zaštitne mjere za prvi scenarij, s obzirom na članke 25. i 32. OUZP--a.

Opis scenarija

35. U prvom scenariju, upisani biometrijski predložak svakog putnika, koji je pristao na takvu obradu, pohranjuje se samo kod pojedinca, na primjer na osobnom uređaju koji nosi svaki putnik nad kojim samo on ima kontrolu. Putnici se autentificiraju (usporedba 1:1) kad prolaze kroz određene kontrolne točke u zračnoj luci.

36. Upis obavlja upravitelj zračne luke, bilo na daljinu putem aplikacije upravitelja zračne luke[51] ili na terminalima zračne luke s odgovarajućom razinom provjere identiteta (npr. eIDAS odgovarajuća razina provjere[52]). Takav upis sastoji se od bilježenja biometrijskog predloška i identifikacijskih podataka na putnikovu uređaju[53] (dalje u tekstu „**ID**") nužnih za obradu. Upis se obavlja samo jednom i to za određeno razdoblje valjanosti (na primjer, usklađeno s razdobljem valjanosti putovnice putnika). Upravitelj zračne luke ne zadržava osobne iskaznice putnika niti njihove biometrijske podatke nakon postupka upisa.

---

[46] Predmet C-439/19 *Latvijas Republikas Saeima*, točke 110. i 113.; Presuda Suda (veliko vijeće) od 4. srpnja 2023., predmet Komisija/EDF, C-252/21 P, ECLI:EU:C:2023:537, točka 108.

[47] Predmeti C-708/18 *M5A-ScaraA*, točke 52.–56., C-92/09, C-93/09 *Volker und Schecke*, točka 87. i C-439/19 *Latvijas Republikas Saeima*, točke 98., 110., 113. Vidjeti i Mišljenje 3/2012 Radne skupine iz članka 29. o biometrijskim tehnologijama, str. 8.

[48] Kao alternativu, pojedinac bi mogao ispisati i pohraniti svoj biometrijski predložak na papir.

[49] Time se ne dovodi u pitanje ukupna odgovornost voditelja obrade za obradu.

[50] Kao što je vidljivo iz primjera uporabe br. 1 u Prilogu I. zahtjeva.

[51] EDPB napominje da bi se u budućnosti mogli predvidjeti alternativni načini takvog upisa i da bi se upis mogao provoditi bez posebne aplikacije upravitelja zračne luke, primjerice interakcijom s digitalnom lisnicom korisnika.

[52] Okvir za elektroničku identifikaciju i usluge povjere (dalje u tekstu „**eIDAS**") na temelju Uredbe (EU) 2024/1183 Europskog parlamenta i Vijeća od 11. travnja 2024. o izmjeni Uredbe (EU) br. 910/2014 u pogledu uspostave europskog okvira za digitalni identitet.

[53] Za potrebe ovog mišljenja, identifikacijski podaci označavaju podatke, kao što su prezime, ime, datum rođenja itd., za koje je potvrđeno da su točni uvidom u osobnu iskaznicu ili putovnicu.

37. Posebno kad je riječ o pohrani, osobna iskaznica i biometrijski predložak putnika pohranjuju se lokalno na uređaju svakog putnika (npr. mobilna aplikacija upravitelja zračne luke ili aplikacija za digitalni novčanik). Uređaj se zatim može koristiti za slanje ili pretraživanje identifikacijske isprave putnika i biometrijskog predloška te može uključivati informacije o letu i/ili kartu za ukrcaj u zrakoplov. Na primjer, te su informacije šifrirane ključem koji posjeduje samo upravitelj zračne luke, koji može biti šifriran u obliku QR koda, koji se može ispisati na papiru ili prikazati na zaslonu uređaja putnika. U tom bi slučaju putnik predočio taj QR na posebnom kontrolnom samoposlužnom uređaju u zračnoj luci s QR skenerom i kamerom.

38. Kad je riječ o sigurnosti, tijekom uparivanja QR kodovi se dešifriraju ključem koji posjeduje operator zračne luke, jedini koji može dešifrirati QR kodove. Biometrijski podaci putnika čuvaju se samo tijekom vrlo kratkog razdoblja i brišu se nakon što se završi uspoređivanje biometrijskih podatka. Treba napomenuti da sigurnosne mjere u pogledu pohrane djelomično ovise o sigurnosti uređaja putnika.

Procjena EDPB-a

39. U prvom scenariju opisuju se tehničke i organizacijske mjere osmišljene kako bi se osigurala razina sigurnosti primjerena rizicima za ispitanike u skladu s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a. Putnici se autentificiraju (usporedba 1:1) kada prolaze kroz određene kontrolne točke u zračnoj luci. U tom se scenariju glavna operacija podudaranja provodi u kontekstu kontroliranog okruženja[54], gdje su putnici aktivno uključeni i imaju veći nadzor nad svojim podacima. Konkretno, provjeravali bi se samo putnici koji su pristali na takvu obradu i, s obzirom na to da bi ih se provjeravalo na posebnim samoposlužnim uređajima, ne bi se prikupljali biometrijski podaci drugih putnika koji nisu pristali na takvu obradu. Osim toga, putnici koji su dali privolu imaju mogućnost u bilo kojem trenutku zaustaviti obradu brisanjem podataka sa svog uređaja.

40. Upotreba prepoznavanja lica na temelju biometrijskog predložaka pohranjenog samo kod pojedinca, koji se, na primjer, može nalaziti na osobnom uređaju koji posjeduje putnik nad kojim samo on ima kontrolu i koji se koristi za autentifikaciju na određenim kontrolnim točkama putem posebnog sučelja, pod određenim uvjetima predstavlja manji rizik u usporedbi s upotrebom biometrijskih podataka ako su podaci pohranjeni u središnjoj bazi podataka[55]. Takva lokalizirana pohrana, ako je popraćena odgovarajućim zaštitnim mjerama[56], smanjuje ozbiljnost povreda osobnih podataka u usporedbi s centraliziranom pohranom kad je riječ o broju pogođenih pojedinaca i osigurava da je za pristup biometrijskom predlošku potrebno aktivno sudjelovanje ispitanika.

41. Nadalje, uspoređivanje bi se moglo provesti lokalno u zračnoj luci usporedbom biometrijskog predloška, na primjer sadržanog u QR kodu, s rezultatom predloška izračunatim na temelju biometrijskog uzorka snimljenog kamerom kontrolnog samoposlužnog uređaja. Kontrolor koji obavlja posebnu provjeru (koja može biti upravitelj zračne luke ili zračni prijevoznik, ovisno o tome obavlja li se na zaštitnim kontrolnim točkama u zračnoj luci, pri predaji prtljage, ukrcaju i/ili pristupu salonu za

[54] „Nekontrolirano okruženje" odnosi se na upotrebu prepoznavanja lica za identifikaciju bez aktivnog sudjelovanja ispitanika, pri čemu se predložak svakog lica koje ulazi u područje praćenja uspoređuje s predlošcima iz širokog poprečnog presjeka stanovništva pohranjenima u bazi podataka, vidjeti Smjernice EDPB-a 5/2022 o prepoznavanju lica u području izvršavanja zakonodavstva, točka 17.

[55] Smjernice EDPB-a 5/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva, točka 17.

[56] Kao što je navedeno u nastavku u točki 46.

putnike) bio bi upoznat samo s rezultatom podudaranja i upotrijebio bi ga. Osim toga, činjenica da informacije potrebne za uspoređivanje biometrijskih podatka (npr. QR kod) moraju dati pojedinci djeluje kao drugi čimbenik[57] čime se povećava sigurnost autentifikacije.

42. Kad je riječ o usklađenosti s člankom 25. OUZP-a, a posebno kako bi se ispunio zahtjev smanjenja količine podataka, trebalo bi osigurati da obrada ispunjava načelo nužnosti. U prvom scenariju moglo bi se smatrati da su odabrane mjere ispunile načelo nužnosti u odnosu na željenu svrhu (tj. ubrzavanje protoka putnika) ako, ovisno o okolnostima obrade, voditelj obrade može dokazati da ne postoje manje nametljiva alternativna rješenja kojima bi se isti cilj mogao učinkovito ostvariti. Na primjer, voditelj obrade može dokazati da, čak i ako bi putnici morali pokazati svoj uređaj, prvi scenarij ubrzava postupak provjere u usporedbi s trenutačnom situacijom koja uključuje provjeru odgovara li ime na karti za ukrcaj u zrakoplov identifikacijskoj ispravi putnika koju provodi čovjek[58]. Konkretno, to se nije moglo dokazati ako trenutačno ne postoje provjere identiteta putnika na temelju njihove službene identifikacijske isprave (u tom pogledu vidjeti prethodnu točku 18.).

43. Osim toga, upravitelj zračne luke ne zadržava biometrijske predloške nakon unosa, a voditelj obrade koji provodi provjeru pohranjuje biometrijske podatake vrlo kratko jer se takvi podaci brišu čim se završi uspoređivanje. Stoga se čini da mjere odabrane u prvom scenariju ograničavaju opseg obrade i razdoblje pohrane osobnih podataka.

44. Kad je riječ o načelu proporcionalnosti, nametljivost takve obrade može se nadoknaditi aktivnim sudjelovanjem putnika jer bi se njihovi biometrijski podaci pohranjivali samo kod njih. Osim toga, uzimajući u obzir prethodno opisane mjere i pod pretpostavkom da voditelj obrade provodi odgovarajuće zaštitne mjere koje se zahtijevaju predmetnom posebnom obradom, provedbom odgovarajućih mjera mogla bi se osigurati razina sigurnosti primjerena riziku. U tom bi se slučaju negativan učinak na temeljna prava i slobode ispitanika mogao smatrati proporcionalnim očekivanoj koristi.

45. Stoga, uzimajući u obzir prethodno navedeno, u odgovoru na pitanje 1.1. Odbor zaključuje da se takva obrada **mogla smatrati načelno usklađenom s člankom 5. stavkom 1. točkom (f), člancima 25. i 32. OUZP-a, pod uvjetom da su poduzete odgovarajuće zaštitne mjere**.

Odgovarajuće zaštitne mjere

46. U toj vrsti scenarija, u odgovoru na pitanje 1.2., EDPB smatra da bi trebalo provesti barem sljedeće zaštitne mjere. Druge zaštitne mjere osim onih opisanih u ovom mišljenju mogle bi se upotrijebiti za postizanje istih ciljeva sigurnosti i zaštite podataka te bi mogle biti zakonite pod uvjetom da se njima osigurava usklađenost s primjenjivim pravnim okvirom.

47. Napomena: to je neiscrpan pregled mogućih odgovarajućih zaštitnih mjera na visokoj razini koje bi voditelj obrade trebao provesti u rješenju sličnom prvom scenariju. Njihova primjerenost u skladu s člancima 25. i 32. OUZP-a ovisit će o analizi svakog pojedinačnog slučaja. Svi voditelji obrade morat će

[57] Na primjer, time se smanjuje rizik od lažnog predstavljanja. Vidjeti i zaštitnu mjeru C.1.2. u nastavku.
[58] Moglo bi se tvrditi da bi biometrijska provjera mogla biti manje podložna pogreškama nego provjera koju provodi čovjek.

provesti vlastitu procjene učinka na zaštitu podataka[59], a za njihova konkretna rješenja mogu biti potrebne dodatne mjere koje nisu uključene u ovo mišljenje.

A. Općenito

A.1. Procjena učinka obrade podataka

A.1.1. Provesti procjenu učinka na zaštitu podataka u skladu s člankom 35. OUZP-a kad god voditelj obrade planira novi postupak obrade koji će vjerojatno prouzročiti visok rizik. To će vjerojatno biti slučaj s prvim scenarijem jer uključuje opsežnu obradu biometrijskih podataka[60]. Procijeniti primjerenost provedbe sustava za prepoznavanje lica, uključujući njegovu nužnost i proporcionalnost u odnosu na željene svrhe[61] u ranoj faze izrade i preispitivati je tijekom cijelog životnog ciklusa razvoja proizvoda.

A.1.2. Zatražiti savjet relevantnog nadzornog tijela ako obrada i dalje predstavlja visoki rizik unatoč mjerama koje je voditelj obrade poduzeo za ublažavanje rizika[62].

A.2. Prava ispitanika i zaštitne mjere koje voditelji obrade mogu primijeniti

A.2.1. Zaštitne mjere za rješavanje slučajeva lažno negativnih rezultata. Kako biste ublažili rizik od dobne, rodne i rasne pristranosti trebate „redovito procjenjivati funkcioniraju li algoritmi u skladu s predviđenim svrhama te prilagođavati algoritme kako bi se ublažio učinak otkrivenih pristranosti i osigurala poštena obrada”[63]. Na primjer, primjenom ljudskog nadzora i intervencije kako bi se ublažile bilo kakve pristranosti i osiguralo da nema stigmatizacije ili profiliranja putnika.

A.2.2. Osigurati da sva obrada osobnih podataka bude transparentna te da su pojedinci upoznati s načinom na koji se njihovi podaci obrađuju i imaju kontrolu nad njim za svaki postupak obrade[64].

A.2.3. Osigurati da su uspostavljene mjere za poštovanje načela ograničenja svrhe kako se podaci ne bi upotrebljavali za druge potrebe, kao što su sigurnosne svrhe ili svrhe osposobljavanja.

A.2.4. Koristiti odgovarajuće mjere koje osiguravaju da se ne snimaju pojedinci koji ne pristanu na prepoznavanje lica (kao što je upotreba odgovarajuće dubine polja i područja snimanja

[59] Članak 35. OUZP-a.
[60] Članak 35. stavak 3. OUZP-a i Smjernice Radne skupine iz članka 29. o procjeni učinka na zaštitu podataka i utvrđivanju vjerojatnosti da će obrada „prouzročiti visok rizik” u smislu Uredbe 2016/679, donesene 13. listopada 2017., WP248rev.01, odobrio EDPB.
[61] Članak 35. stavak 7. točka (b) OUZP-a.
[62] Članak 36. stavak 1. OUZP-a.
[63] Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., bilješka 60., točka 70.
[64] Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., točka 68. i uvodna izjava 7. OUZP-a.

kako bi se izbjeglo snimanje drugih putnika u pozadini ili blizini, uvođenje posebnih redova koji su jasno označeni za prepoznavanje lica), čak i ako se fotografije i videozapisi ne pohranjuju niti obrađuju.

A.2.5. Ako iste samoposlužne uređaje mogu koristiti putnici koji su pristali i oni koji nisu pristali na upotrebu prepoznavanje lica ili ako se putnici koji nisu pristali na prepoznavanje lica mogu pojaviti u vidnom polju dok se sustav ne upotrebljava, pričekajte da vam putnik koji je dao privolu prije početka snimanja fotografije ili videozapisa da znak.

A.2.6. Mogućnost da ispitanik u bilo kojem trenutku izbriše podatke koji su samo kod njega (biometrijski predložak)[65] u mobilnoj aplikaciji ili digitalnom novčaniku[66].

A.2.7. Postojanje održivih alternativa ili rezervnih rješenja (tj. za putnike koji ne pristanu na upotrebu svojih biometrijskih podataka, za putnike koji ne bi mogli upotrebljavati takva rješenja ili za putnike koji su pogrešno odbijeni) kako bi se također osiguralo da putnici koji ne pristanu nemaju nikakve posljedice[67].

A.2.8. Ako se aplikacija koristi, trebala bi biti pažljivo osmišljena i konfigurirana kako se ne bi prikupljali nepotrebni podaci i kako bi se izbjeglo korištenje kompleta za razvoj softvera trećih strana („SDK") koji prikupljaju podatke u druge svrhe.

A.3 Odgovornost

A.3.1. Procijeniti postoje li relevantni kodeksi ponašanja ili mehanizmi certificiranja koji pomažu u dokazivanju usklađenosti sa sigurnošću obrade iz članka 32. OUZP-a[68]. Provjerite prikladnost mjera za predmetnu obradu. Standardi[69] najbolje prakse i kodeksi ponašanja koje priznaju udruženja i druga tijela koja predstavljaju kategorije voditelja obrade mogu vam pomoći utvrditi odgovarajuće mjere.

A.3.2. Osigurati osnovne sigurnosne provjere uređaja korisnika kako bi se omogućila faza upisa, iako putnik također ima ulogu u zaštiti svojih podataka jer su pohranjeni na njegovu uređaju. Primjeri takvih tehničkih provjera i kontrola prikazani su u nastavku u odjeljku C.2. „Infrastruktura i mreža".

B. Organizacijski:

B.1. Politika i usklađenost

[65] Upućivanja na biometrijski predložak u zaštitnim mjerama za prvi scenarij odgovaraju upućivanjima na ključ/lozinku u drugom scenariju.
[66] Imajte na umu da se ova zaštitna mjera primjenjuje samo na prvi scenarij.
[67] Smjernice EDPB-a 3/2019 o videouređajima, točka 86.
[68] Članak 32. stavak 3. OUZP-a i Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., točka 10.
[69] Vidjeti, na primjer, ISO/IEC 2382-37.

B.1.1. Uspostavite unutarnje kontrole pristupa[70] s pravilima za administratore.

B.1.2. Ako uslugu prepoznavanja lica mogu pružiti druge strane uključene u obradu bez osobne iskaznice ili biometrijskih podataka, ili obiju vrsta podataka, zabranjuje se protok tih podataka preko tih drugih uključenih strana. Na primjer, zračni prijevoznik ne mora tehnički pristupiti biometrijskim podacima kad koristi zajedničku infrastrukturu zračne luke, čak i ako taj zračni prijevoznik djeluje kao voditelj obrade na temelju OUZP-a.

B.1.3. Definirati pravila za šifriranje i upravljanje ključevima[71], primjerice za obradu osobnih i biometrijskih podataka.

B.1.4. Osigurati usklađenost s Poglavljem V. OUZP-a. Na primjer, kako bi se osigurala usklađenost prijenosa ako se voditelj obrade tijekom postupka upisa koristi uslugom na daljinu sa sjedištem u trećoj zemlji.

B.1.5. Kad se koriste izvršitelji obrade, treba sklopiti ugovor o izvršitelju obrade[72] u skladu s člankom 28. stavkom 3. OUZP-a.

B.1.6. Uspostaviti postupke za upravljanje ljudskim nadzorom i intervencijom, posebno za rješavanje problema pogrešnog odbijanja te tehničkih problema ili problema u pogledu upotrebljivosti.

B.2 Osposobljavanje i testiranje

B.2.1.Osigurati da je osoblje osposobljeno na odgovarajući način.

B.2.2. Provoditi „proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade”[73].

B.2.3. Provesti postupak kojim se osigurava da je obrada biometrijskog predložaka putnika[74] za autentifikaciju tehnički učinkovita i dovoljno precizna:

B.2.4. Osigurajte da su biometrijski uzorci prikupljeni pri upisu i na kontrolnoj točki dovoljno kvalitetni za pouzdanu biometrijsku obradu.

C. Tehnički:

[70] Smjernice EDPB-a 04/2020 o upotrebi podataka o lokaciji i alatima za praćenje kontakata u kontekstu pandemije bolesti COVID-19, donesene 21. travnja 2020. (dalje u tekstu „**Smjernice Europskog odbora za zaštitu podataka 4/2020 o podacima o lokaciji i alatima za praćenje kontakata**”), SEC-10, str. 16.
[71] Smjernice EDPB-a 3/2019 o videouređajima, točka 89.
[72] Članak 28. stavak 3. OUZP-a.
[73] Članak 32. stavak 1. točka (d) OUZP-a.
[74] Upućivanja na biometrijski predložak u zaštitnim mjerama za prvi scenarij odgovaraju upućivanjima na ključ/lozinku u drugom scenariju.

C.1 Pristup

C.1.1. Provesti zaštitne mjere tijekom faze upisa kako bi se osigurao postupak upisa primjenom ponovljenog uzorkovanja (metoda bootstrap) s potvrđenim identitetom. Na primjer, kako bi se pojačala procjena identiteta korisnika putem višefaktorske autentifikacije, mogu se provesti koraci, od jednokratnih poveznica zaštićenih lozinkom za aktivaciju aplikacije do lokalnih mehanizama za deblokiranje uređaja.

C.1.2. Provesti zaštitne mjere kako bi se uzeli u obzir slučajevi lažno pozitivnih rezultata, napada korištenjem lažnih biometrijskih karakteristika i sprečavanje prijevara[75].

C.1.3. Zabrana bilo kakvog vanjskog pristupa osobnim i biometrijskim podacima[76].

C.1.4. Osigurati da se obrada obavlja lokalno u fazama upisa, prijenosa i uspoređivanja biometrijskih podataka. Točka podudaranja trebala bi biti što bliža uređaju pojedinca. Za omogućavanje uparivanja predložaka unutar pojedinačnog uređaja mogla bi biti potrebna interakcija s pružateljima usluga koji se nalaze izvan zračne luke i uključivati upotrebu javnih mrežnih resursa, a nedostatak toga je utjecaj na dostupnost i dijeljenje predloška s vanjskim subjektima.

C.1.5. Autentificirati korisnika za dodavanje novog leta i generiranje novog šifriranog QR koda.

C.1.6. Provesti mjere za rješavanje situacije u kojoj putnik može izgubiti pristup svom QR kodu.

C.2. Infrastruktura i mreža

C.2.1. Uvjeti za operativni sustav moraju biti ažuriran, a autentifikacija za pristup uređaju omogućena kako bi aplikacija / digitalni novčanik funkcionirao, uključujući automatsko brisanje osobnih i biometrijskih podataka ako je operativni sustav zastario i predstavlja sigurnosni rizik.

C.2.2. Izolirati jedinice za uspoređivanje biometrijskih podataka (samoposlužne uređaje) dok su u funkciji i poduzeti sve druge mjere potrebne kako bi se osigurala sigurnost.

C.2.3. Provoditi uspoređivanja biometrijskih podataka na putnikovom uređaju ili na samoposlužnom uređaju (računalstvo na rubu mreže).

C.2.4. Rješenja za otklanjanje sigurnosnih ranjivosti pojedinačnih uređaja putnika, uključujući šifriranje (najmanje) biometrijskih i osobnih podataka u mirovanju.

[75] Izvješće ENISA-e o digitalnom identitetu o iskorištavanju koncepta identitet kojim korisnik upravlja bez posrednika (SSI) za izgradnju povjerenja iz siječnja 2022.
[76] Smjernice EDPB-a 3/2019 o videouređajima, točka 89.

C.2.5. Koristiti sigurnu pohranu za (barem) biometrijske podatke koji se nalaze samo kod korisnika[77], primjerice upotrebom sigurne enklave na pametnom telefonu.

C.2.6. Zaštitne mjere za osiguranje fizičke sigurnosti prostora, uključujući biometrijski terminal zračne luke. Osigurati visoku razinu sigurnosti elemenata arhitekture koji obrađuju (npr. računanje, protok podataka, privremena ili dugoročna pohrana) osobne i biometrijske podatke.

C.3. Sigurnost i upravljanje podacima za provjeru identiteta korisnika

C.3.1. Podijeliti podatke tijekom prijenosa i pohrane u najmanje tri različite skupine, kao što su: osobna iskaznica, biometrijski podaci i podaci o letu[78]. Osigurati odgovarajuće šifriranje podataka tijekom prijenosa i pohrane;

C.3.2. Uspostaviti tehničke mjere kako bi se osiguralo da se na određenoj kontrolnoj točki obrađuju i provjeravaju samo podaci koji se mogu zakonito obrađivati.

C.3.3. Osigurati učinkovitost brisanja podataka[79] sigurnim postupkom brisanja (na primjer, glavna memorija, predmemorija, moguće sigurnosne kopije) i procijeniti kada bi brisanje podataka trebalo automatizirati. Razdoblja pohrane podataka trebala bi se strogo primjenjivati automatskim postupcima bez potrebe za dodatnim djelovanjem pojedinca[80].

C.3.4. Osigurati vjerodostojnost i cjelovitost podataka (na primjer, potpis)[81].

C.3.5. Biometrijske podatke putnika na ulaznoj i kontrolnoj točki zadržati samo na vrlo kratko vrijeme i izbrisati ih čim putnik prođe kroz kontrolnu točku;

C.3.6. Ako se za upis koristi aplikacija, pri razvoju aplikacija primijenite sigurnosne standarde za sigurnost mobilnih aplikacija i sigurnosne testove treće strane.

C.3.7. Primijeniti sigurnosne mjere tijekom faze upisa u zračnoj luci kako bi se zaštitila povjerljivost i cjelovitost biometrijskih podataka putnika. Na primjer, ako se QR kod ispisuje na kiosku, QR kod ne bi se trebao prikazivati na kiosku kako ga ne bi mogao fotografirati zlonamjerni. Kad je riječ o prijenosu kratkog dometa, u prijenos bi trebao aktivno sudjelovati korisnik te bi se trebao obavljati putem kanala koji osigurava blizinu.

[77] Upućivanja na biometrijski predložak u zaštitnim mjerama za prvi scenarij odgovaraju upućivanjima na ključ/lozinku u drugom scenariju.
[78] Smjernice EDPB-a 3/2019 o videouređajima, točka 89.
[79] Smjernice EDPB-a 3/2019 o videouređajima, točka 89.
[80] Smjernice 4/2019 o tehničkoj i integriranoj zaštiti podataka iz članka 25., str. 82.
[81] Smjernice EDPB-a 3/2019 o videouređajima, točka 89.

C.3.8. Podaci koji se nalaze samo kod pojedinca[82] moraju se čuvati u sigurnoj memoriji na njegovu uređaju, a na sve moguće ranjivosti povezane s operativnim sustavima uređaja moraju se primijeniti odgovarajuće sigurnosne zakrpe. Kad je riječ o tiskanom QR kodu, pojedinac bi trebalo upoznati s osobito osjetljivom prirodom podataka koje sadržava i onoga što omogućuje.

C.3.9. Osigurajte da se upis provodi u skladu s odgovarajućim tehnikama provjere identiteta na daljinu[83].

3.2.2. Scenarij 2.: centralizirana pohrana upisanog biometrijskog predloška u šifriranom obliku unutar zračne luke s ključem/lozinkom koju posjeduje samo putnik, radi autentifikacije

48. U ovom se odjeljku ispituje usklađenost s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a centralizirane pohrane biometrijskih predložaka putnika radi autentifikacije u centraliziranoj bazi podataka, u šifriranom obliku i s ključem/lozinkom koji posjeduje samo putnik[84] (dalje u tekstu „**drugi scenarij**"). U ovom se odjeljku ispituju i odgovarajuće zaštitne mjere za drugi scenarij, s obzirom na članke 25. i 32. OUZP-a.

Opis scenarija

49. U drugom scenariju, upis se obavlja samo jednom, tijekom određenog razdoblja valjanosti (na primjer, godinu dana nakon posljednjeg leta, sve do isteka valjanosti putovnice), na daljinu na odgovarajućoj razini osiguranja identiteta (npr. odgovarajuća razina osiguranja eIDAS-a) ili na terminalima zračnih luka. Upis kontrolira upravitelj zračne luke i sastoji se od generiranja osobnih i biometrijskih podataka koji su šifrirani ključem/lozinkom.

50. Baza podataka pohranjena je u prostorijama zračne luke pod kontrolom upravitelja zračne luke. Kjučevi/lozinke za šifriranje za konkretnog pojedinca pohranjuju se samo na njegovu uređaju (primjerice u mobilnoj aplikaciji upravitelja zračne luke). Aplikacija može generirati QR kod koji sadrži ključ/lozinku, koji se može ispisati na papiru ili prikazati na zaslonu uređaja[85]. Osim toga, drugi sloj šifriranja[86] obavlja upravitelj zračne luke s ključevima koje on kontrolira.

51. Putnici se autentificiraju (usporedba 1:1) kada prolaze kroz određene kontrolne točke u zračnoj luci. Putnici koji odluče proći kroz biometrijske kontrolne točke pokazuju svoj QR kod na posebnom kontrolnom samoposlužnom uređaju s QR skenerom i kamerom. Indeks putnika šalje se u bazu podataka kako bi se zatražio šifrirani predložak koji se preuzima i provjerava lokalno na

[82] Upućivanja na biometrijski predložak u zaštitnim mjerama za prvi scenarij odgovaraju upućivanjima na ključ/lozinku u drugom scenariju.
[83] Pogledajte izvješće ENISA-e o provjeri identiteta na daljinu: Analiza metoda za provjeru identiteta na daljinu, ožujak 2021.
[84] Kao što je vidljivo iz primjera uporabe br. 2 u Prilogu I. Zahtjeva.
[85] Francusko nadzorno tijelo dodatno je pojasnilo da bi mogla postojati i druga tehnička rješenja za slanje potrebnih informacija, poput upotrebe komunikacijskog protokola kratkog dometa.
[86] Ključ/lozinka (koju posjeduje pojedinac) šifriran je drugim ključem koji posjeduje upravitelj zračne luke.

samoposlužnom i/ili korisničkom uređaju. Kontrolor na kontrolnoj točki dobiva i koristi samo utvrđene podudarnosti[87].

52. U tom scenariju ne postoji protok osobnih i biometrijskih podataka među zračnim lukama, a centralizirane baze podataka nisu međusobno povezane ni interoperabilne.

Procjena EDPB-a

53. U drugom scenariju biometrijski predlošci koje su putnici unijeli pohranjuju se centralizirano, ali u šifriranom obliku i s ključem/lozinkom koju posjeduje samo putnik. U drugom scenariju putnici se autentificiraju (usporedba 1:1).

54. U tom se scenariju predlaže da bi se cilj ubrzavanja protoka putnika (tj. povećanjem brzine provjera) mogao postići upotrebom centraliziranog sustava. EDPB prethodno je napomenuo da bi se takvo rješenje moglo smatrati održivom alternativom decentraliziranoj pohrani upisanih biometrijskih predložaka[88] (kako je opisano u prvom scenariju), ako postoje objektivne potrebe i uz primjenu odgovarajućih zaštitnih mjera (vidjeti zaštitne mjere opisane u točki 60. u nastavku).

55. Kad je riječ o sigurnosnim pitanjima, podaci svakog pojedinca šifriraju se posebnim ključem koji se nalazi samo kod njega i nad kojim samo on ima kontrolu. Nadalje, činjenica da informacije potrebne za uspoređivanje biometrijskih podataka (tj. ključ/lozinka) mora dati pojedinac djeluje kao drugi čimbenik[89] čime se povećava sigurnost autentifikacije. Osim toga, drugi sloj šifriranja obavlja upravitelj zračne luke s ključevima koje on kontrolira. U drugom scenariju, indeks pojedinca šalje se u središnju bazu podataka kako bi se dobili biometrijski podaci povezani s njime. Ti se podaci zatim šalju (šifrirani) na računalo na kontrolnoj točki gdje se dešifriraju kako bi se usporedili biometrijski podataci, a voditelj obrade kontrolne točke zna i upotrebljava samo utvrđene podudarnosti. Pod uvjetom da se pojedinčev ključ/lozinka čuva u računalu smještenom na kontrolnoj točki i da se u središnju bazu podataka šalje samo indeks putnika radi pronalaženja šifriranog biometrijskog predloška, takve bi se sigurnosne mjere stoga mogle smatrati usklađenima s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a.

56. Kad je riječ o usklađenosti s člankom 25. OUZP-a, a posebno kako bi se ispunio zahtjev smanjenja količine podataka, trebalo bi osigurati da obrada ispunjava načelo nužnosti. U drugom scenariju moglo bi se smatrati da su odabrane mjere ispunile načelo nužnosti u odnosu na željenu svrhu (tj. ubrzavanje protoka putnika u zračnim lukama) ako, ovisno o okolnostima obrade, voditelj obrade može dokazati da ne postoje manje nametljiva alternativna rješenja kojima bi se isti cilj mogao učinkovito ostvariti. U drugom scenariju putnici će i dalje morati pokazati svoj uređaj[90]. Međutim, voditelj obrade može dokazati da drugi scenarij ubrzava postupak provjere u usporedbi s trenutačnom situacijom koja

[87] Francusko nadzorno tijelo pojasnilo je da je to razdoblje pohrane ilustrativno i da se može smatrati prihvatljivim s obzirom na to da se ključ nalazi kod pojedinaca i da se može odabrati u fazi upisa. Međutim, treba napomenuti da se razdoblje pohrane može prilagoditi.

[88] Smjernice EDPB-a 3/2019 o videouređajima, točka 88.

[89] Na primjer, time se smanjuje rizik od lažnog predstavljanja. Vidjeti također zaštitnu mjeru C.1.2.

[90] Francusko nadzorno tijelo dodatno je pojasnilo da bi mogle postojati i druge mogućnosti za predočavanje predloška, primjerice tiskanog na papiru. Osim toga, EDPB uviđa da bi se u budućnosti mogla predvidjeti upotreba alternativne tehnologije, npr. na temelju sustava komunikacije s malom udaljenošću.

uključuje provjeru odgovara li ime na karti za ukrcaj u zrakoplov identifikacijskoj ispravi putnika[91] koju provodi čovjeke ili u usporedbi s prvim scenarijem. Konkretno, to se nije moglo dokazati ako trenutačno ne postoje provjere identiteta putnika na temelju njihove službene identifikacijske isprave (u tom pogledu vidjeti prethodnu točku 18.).

57. Kad je riječ o načelu proporcionalnosti, nametljivost takve obrade može se kompenzirati aktivnim sudjelovanjem putnika, koji jedini posjeduju ključ za svoje šifrirane podatke. Osim toga, čini se da se sigurnosni rizici povezani s pohranom biometrijskih podataka putnika u središnjoj bazi podataka i s ključem koji posjeduje samo putnik mogu ublažiti primjenom odgovarajućih zaštitnih mjera (vidjeti zaštitne mjere navedene u točki 60. u nastavku). Stoga, pod pretpostavkom da voditelj obrade provodi odgovarajuće zaštitne mjere koje zahtijeva predmetna obrada, rizici za pojedince mogli bi se ublažiti, a negativan učinak na temeljna prava i slobode ispitanika mogao bi se smatrati proporcionalnim očekivanoj koristi. Naravno, u svakom slučaju treba osigurati da se obrađuju samo podaci potrebni za tu svrhu i da se provjeravaju samo putnici koji su dali privolu, tako da ne postoji rizik da će se prikupljati biometrijski podaci drugih putnika koji nisu dali privolu.

58. U zahtjevu se kao primjer navodi da bi u drugom scenariju razdoblje pohrane šifriranih podataka u bazi podataka obično moglo biti godinu dana nakon posljednjeg leta pojedinca i do isteka valjanosti putovnice. U zahtjevu nisu navedene informacije koje bi objektivno opravdale tako dugo razdoblje, iako se može pretpostaviti da je takvo razdoblje pohrane predviđeno iz praktičnih razloga za buduće letove. Kad je riječ o razdoblju pohrane, kako bi se u tom scenariju postigla usklađenost s člankom 5. stavkom 1. točkom (e) OUZP-a, voditelji obrade trebali bi moći obrazložiti zašto je to razdoblje potrebno za određenu svrhu u konkretnim slučajevima. Odbor preporučuje voditeljima obrade da predvide najkraće moguće razdoblje pohrane, uzimajući u obzir i putnike koji lete vrlo rijetko, te da ispitanicima ponude da odrede željeno razdoblje pohrane.

59. Uzimajući u obzir prethodno naveden kao odgovor na pitanje 2.1.1. Odbor zaključuje da bi se takva obrada **mogla smatrati načelno usklađenom s člankom 5. stavkom 1. točkom (e), člankom 5. stavkom 1. točkom (f), člancima 25. i 32. OUZP-a, pod uvjetom da su uspostavljene odgovarajuće zaštitne mjere.**

Odgovarajuće zaštitne mjere

60. U toj vrsti scenarija Odbor kao odgovor na pitanje 2.1.2. smatra kako bi **uz zaštitne mjere navedene u prvom scenariju**, trebalo provesti barem sljedeće zaštitne mjere. Druge zaštitne mjere osim onih opisanih u ovom mišljenju mogle bi se upotrijebiti za postizanje istih ciljeva sigurnosti i zaštite podataka te bi mogle biti zakonite pod uvjetom da se njima osigurava usklađenost s primjenjivim pravnim okvirima.

61. Napomena: *to je neiscrpan pregled mogućih odgovarajućih zaštitnih mjera na visokoj razini koje bi voditelj obrade mogao provesti u rješenju sličnom drugom scenariju. Njihova primjerenost u skladu s člancima 25. i 32. OUZP-a ovisit će o analizi svakog pojedinačnog slučaja. Svi voditelji obrade morat će provesti vlastitu procjene učinka na zaštitu podataka, a za njihova konkretna rješenja mogu biti potrebne dodatne mjere koje nisu uključene u ovo mišljenje.*

[91] Moglo bi se tvrditi da bi biometrijska provjera mogla biti manje podložna pogreškama nego provjera koju provodi čovjek.

D. Općenito

D.1. Prava ispitanika i zaštitne mjere koje voditelji obrade mogu provesti

D.1.1. Osigurajte da putnik ima kontrolu nad razdobljima pohrane svih svojih podataka. Razdoblja pohrane trebala bi biti ograničena na ono što je nužno za posebnu svrhu. Nakon temeljite analize čimbenika kao što je valjanost identifikacijskog dokumenta, trebalo bi odrediti maksimalno razdoblje. Ispitanicima bi trebalo ponuditi da odrede željeno razdoblje pohrane, koje bi moglo biti kraće od unaprijed utvrđenog razdoblja pohrane.

D.1.2. Mogućnost da ispitanik u bilo kojem trenutku zatraži brisanje podataka koji se nalaze samo kod njega (ključ/lozinka) pohranjeni u mobilnoj aplikaciji ili digitalnom novčaniku[92].

D.1.3. Osigurati da smještaj središnje baze podataka omogućuje stvarni nadzor nadležnog nadzornog tijela.

E. Organizacijski:

E.1 Politike i usklađenost

E.1.1. Povjerenje u središnji poslužitelj mora biti ograničeno. Središnjim poslužiteljem mora se upravljati u skladu s jasno definiranim pravilima upravljanja te se moraju uvesti sve potrebne mjere kako bi se zajamčila njegova sigurnost[93].

F. Tehnički:

F.1. Pristup

F.1.1. Vođenje evidencije o tome tko ima pristup osobnim podacima, posebno osobnim i biometrijskim podacima, i kada im je pristupljeno.

F.2 Infrastruktura i mreža

F.2.1. Na odgovarajući način osigurati središnju bazu podataka, uključujući zaštitu od napada na dostupnost.

F.2.2. Osigurati da nema internetske veze sa središnjom bazom podataka, jedinicama za upis i odgovarajućim jedinicama. Rad i održavanje tog sustava (npr. sigurnosna kopija, ažuriranje, praćenje itd.) moraju se obavljati lokalno unutar prostora zračne luke.

[92] Imajte na umu da se ova zaštitna mjera primjenjuje samo na drugi scenarij.
[93] Smjernice EDPB-a 4/2020 o podacima o lokaciji i alatima za praćenje kontakata, PRIV-5, str. 17.

F.3 Sigurnost i upravljanje podacima

F.3.1. Uvesti najsuvremenije kriptografske tehnike kako bi se osigurala razmjena između aplikacije i središnjeg poslužitelja[94];

F.3.2. Čuvati pojedinačni ključ/lozinku na razini na kojoj će se upotrebljavati za dešifriranje (tj. u uređaju) i upotrebljavati indeks samo za pronalazak odgovarajućeg upisanog biometrijskog predloška u središnjoj bazi podataka.

F.3.3. Osigurati da je komunikacija pri razmjeni ključa/lozinke između korisničkog i samoposlužnog uređaja zaštićena od svakog mogućeg prisluškivanja ili prijenosa trećim stranama.

F.3.4. Indeksirati biometrijski predložak kad je pohranjen u središnjoj bazi podataka kako biste omogućili autentifikaciju 1:1 i osigurali da je jedinstven i povezan s pojedincem. Osigurati da indeks ne otkriva osobne podatke putnika i da nije povezan s ključem za šifriranje.

F.3.5. Primjereno autentificirati i šifrirati svaki prijenos između središnje baze podataka i kontrolnih točaka te ga provodit na izoliranim mrežama.

F.3.6. Izbjegavajte dvosmjerne veze između skupova podataka (osobni i biometrijski podaci, kao i podaci o letu) i zadržite samo relevantne jednosmjerne veze u bazi podataka. Na primjer, samo jednosmjerne veze od indeksa do osobnih podataka, od indeksa do šifriranih biometrijskih podataka i od indeksa do podataka o letu.

F.3.7. Osigurati mehanizme za kontinuitet poslovanja, primjerice uspostavom odgovarajućih pričuvnih sustava za pohranu podataka.

F.3.8. Osigurati da samoposlužni uređaji ne vode evidenciju šifriranih ili nešifriranih predložaka.

3.2.3. Centralizirana pohrana upisanih biometrijskih predložaka za identifikaciju

62. U ovom se odjeljku ispituje usklađenost centralizirane pohrane biometrijskih predložaka putnika za identifikaciju s člankom 5. stavkom 1. točkama (e) i (f) te člancima 25. i 32. OUZP-a ako ti predlošci nisu šifrirani ključem/lozinkom koju posjeduje samo putnik, u dva slučaja upotrebe: 1. kad su takvi predlošci pohranjeni u bazi podataka unutar zračne luke, pod kontrolom upravitelja zračne luke[95]

[94] Smjernice EDPB-a 4/2020 o podacima o lokaciji i alatima za praćenje kontakata, SEC-4, str. 16.: „Primjeri tehnika koje se mogu primijeniti uključuju: simetričnu i asimetričnu enkripciju, funkcije za izračun sažetka (hash functions), enkripcijske protokole PTM (private membership test), PSI (private set intersection) i PIR (private information retrieval), Bloom filtre, homomorfnu enkripciju itd.

[95] Kao što je vidljivo iz primjera uporabe 3A iz Priloga I. Zahtjevu.

(dalje u tekstu „**scenarij 3.1**”), i 2. kad su takvi predlošci pohranjeni u oblaku, pod kontrolom zračnog prijevoznika[96] (dalje u tekstu „**scenarij 3.2**”).

63. Odbor smatra da uporaba biometrijskih podataka za **identifikacijske** svrhe u velikim središnjim bazama podataka zadire u temeljna prava ispitanika i mogla bi imati ozbiljne posljedice za ispitanike[97]. Osim toga, trebalo bi ispitati i upotrebu biometrijskih podataka u odnosu na svrhu za koju se obrađuju, s obzirom na načela nužnosti i proporcionalnosti[98].

3.2.3.1. Scenarij 3.1.: centralizirano pohranjivanje u bazi podataka unutar zračne luke, pod kontrolom upravitelja zračne luke

Opis scenarija

64. U scenariju 3.1. biometrijski predložak putnika pohranjuje se u središnjoj bazi podataka u prostorijama zračne luke i pod kontrolom je upravitelja zračne luke u šifriranom obliku. Konkretno, podaci o putnicima segmentirani su, što znači da se njihovi osobni podaci, upisani biometrijski predložak i informacije o letu pohranjuju u tri različite baze podataka. Takvi se podaci šifriraju različitim ključevima, kako tijekom pohrane tako i tijekom prijenosa na poslužitelje koji provode uspoređivanje biometrijskih podataka, gdje ih upravitelj zračne luke zatim dešifrira.

65. Putnici se moraju prijaviti za svaki let u kratkom razdoblju prije polaska (npr. 48 sati). Takav se upis može obaviti na daljinu ili na terminalima zračne luke na odgovarajućoj razini osiguranja identiteta (npr. odgovarajuća razina osiguranja eIDAS-a). Alternativno, upis može imati isti oblik kao što je opisano u prvom scenariju, u kojem slučaju putnici moraju prenijeti svoje podatke iz svojih digitalnih novčanika u sustav zračne luke u roku od 48 sati prije polaska.

66. I u ovom scenariju putnici se prijavljuju pred posebnim kontrolnim samoposlužnim uređajem s kamerom. Njihov biometrijski uzorak zatim se šalje na središnji poslužitelj zračne luke, koji će pokušati usporediti podatke s podacima iz središnje biometrijske baze podataka. Putnik se stoga može identificirati i provjeriti je li doista registriran za odlazni let (ili ukrcaj u slučaju kontrole pri ukrcaju). Ovisno o kontrolnoj točki, podaci koji se šalju natrag voditelju obrade kontrolne točke koji podnosi zahtjev mogu se, prema potrebi, svesti na najmanju moguću mjeru, na primjer „da/ne odgovor” ili samu utvrđenu podudarnost. U tom se slučaju voditelju obrade na kontrolnoj točki prenosi samo rezultat zahtjeva te on koristi samo njega.

67. Konkretno, u tom se scenariju putnici se identificiraju (usporedba 1:N), pri čemu je N broj putnika koji se očekuje u zračnoj luci u razdoblju od nekoliko dana. Nadalje, uspoređivanje biometrijskih podataka provodi se samo kada se svaki putnik pojavi na unaprijed definiranim kontrolnim točkama u polaznoj zračnoj luci, dok se sama obrada podataka obavlja na središnjem poslužitelju povezanom sa središnjom bazom podataka. Razdoblje pohrane u ovom scenariju obično je 48 sati, a podaci se brišu nakon polijetanja zrakoplova.

---

[96] Kao što je vidljivo iz primjera uporabe 3B iz Priloga I. Zahtjevu.

[97] Na primjer, vidjeti Mišljenje 3/2012 Radne skupine iz članka 29. o biometrijskim tehnologijama, str. 8. Vidjeti i prethodnu 26 točku.

[98] Uvodna izjava 4. OUZP-a; Vidjeti i Mišljenje 3/2012 Radne skupine iz članka 29. o biometrijskim tehnologijama, str. 8.

Procjena EDPB-a

68. Kako je prethodno navedeno, obrada biometrijskih podataka podrazumijeva povećane rizike za prava i slobode ispitanika[99]. Stoga svaki nedostatak sigurnosti podataka može imati posebno ozbiljne posljedice za ispitanike[100]. Voditelji obrade obvezni su učinkovito ublažavati te rizike. Budući da je u tom scenariju cjelokupna arhitektura potpuno centralizirana, putnici u većoj mjeri gube kontrolu nad svojim podacima. Osim toga, rizik da će se podaci obrađivati u druge svrhe osim kontrole protoka putnika mogao bi biti veći.

69. S obzirom na načelo i zahtjeve u pogledu sigurnosti (članak 5. stavak 1. točka (f) i članak 32. OUZP-a), trebalo bi uzeti u obzir da pohrana osobnih i biometrijskih podataka u središnjim, iako zasebnim, bazama podataka može predstavljati visoko vrijedne točke napada, a povreda povjerljivosti takve baze podataka može omogućiti pristup cijelom skupu podataka. Zbog toga moguća povreda povezana s predlošcima za prepoznavanje lica i povezanim osobnim podacima može omogućiti neovlaštenu ili nezakonitu identifikaciju ispitanika u drugim okruženjima. Ovisno o metodama koje se koriste za biometrijsku identifikaciju, može ugroziti i daljnju sigurnu uporabu predložaka za prepoznavanje lica kao identifikatora. U tom se slučaju učinci povrede ne mogu ublažiti, za razliku od druge vrste vjerodajnica (npr. korisničko ime, lozinka) koji se mogu promijeniti[101].

70. Osim toga, velika količina i kvaliteta osobnih i biometrijskih podataka koje posjeduje voditelj obrade čini ga vrlo vrijednom metom za napadača zbog čega je taj sigurnosti rizik ocijenjen kao znatno vjerojatniji. Osim toga, povrede podataka mogle bi imati veći učinak jer bi zbog pohrane podataka na središnjoj lokaciji napadačima moglo biti lakše pristupiti osobnim podacima većeg broja putnika. Stoga bi moguća povreda mogla izložiti velik broj ispitanika visokim rizicima u smislu ozbiljnosti, na primjer krađa identiteta velikih razmjera, koje je iznimno teško ublažiti.

71. Stoga su kad je riječ o usklađenosti s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a, mjere predviđene u scenariju 3.1.[102], uzimajući u obzir suvremena tehnološka dostignuća nedovoljne osiguranje razine sigurnosti primjerene riziku. Na temelju toga, obrada u okviru scenarija 3.1. ne bi bila u skladu s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a ako bi voditelj obrade koristio samo te mjere.

72. S obzirom na načelo iz članka 5. stavka 1. točke (e) Opće uredbe o zaštiti podataka, u ovom scenariju razdoblje pohrane biometrijskih podataka u središnjoj bazi podataka obično iznosi 48 sati. Čini se da takvo ograničenje pohrane znatno smanjuje rizike povezane s povredama osobnih podataka. Međutim, razdoblje pohrane podataka samo po sebi nije odlučujući čimbenik za ukupnu usklađenost navedene arhitekture jer voditelji obrade mogu izmijeniti takva razdoblja. U svakom slučaju, predložene mjere moraju biti u skladu sa zahtjevima tehničke i integrirane zaštite podataka iz članka 25. Opće uredbe o zaštiti podataka.

73. Za razliku od scenarija 1. i 2., u kojima su putnici autentificirani, u scenariju 3.1. putnici se identificiraju (usporedba 1:N), pri čemu je N broj putnika koji se očekuje u zračnoj luci u razdoblju od nekoliko dana

[99] Vidjeti prethodnu točku 26.
[100] Smjernice za prepoznavanje lica, Savjetodavni odbor Konvencije Vijeća Europe za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka, lipanj 2021., str. 22.
[101] Vidjeti u tom pogledu Mišljenje Radne skupine iz članka 29. o biometrijskim tehnologijama 3/2012, str. 34.
[102] Kako je opisano u točkama od 64. do 67.

i koji su pristali na takvu obradu pri prolasku kroz određene kontrolne točke u zračnoj luci. To podrazumijeva pretraživanje putnika unutar središnje baze podataka obradom svakog uzetog biometrijskog uzorka kako bi se provjerilo podudara li se s osobom poznatom sustavu. Za razliku od drugog scenarija, u scenariju 3.1 ključeve posjeduju samo putnici. Prema tome, u tom scenariju putnici imaju znatno manju kontrolu nad svojim biometrijskim podacima. Stoga takva obrada predložena u scenariju 3.1. ne može biti u skladu sa zahtjevima tehničke i integrirane zaštite podataka na temelju članka 25. OUZP-a.

74. S obzirom na članak 25. OUZP-a, voditelji obrade trebali bi razmotriti vrste, kategorije i razinu detalja osobnih podataka potrebnih za svrhe obrade[103]. Pri odabiru opcija trebali bi uzeti u obzir povećane rizike za načela smanjenja količine podataka, cjelovitosti i povjerljivosti te ograničenja pohrane pri prikupljanju velikih količina detaljnih osobnih podataka, i usporediti ih sa smanjenjem rizika pri prikupljanju manjih količina i/ili manje detaljnih informacija o ispitanicima. U svakom slučaju, zadana postavka ne bi trebala uključivati prikupljanje osobnih podataka koji nisu potrebni za konkretnu svrhu obrade. Drugim riječima, ako su određene kategorije osobnih podataka nepotrebne ili ako detaljni podaci nisu potrebni jer su dostatni manje detaljni podaci, tada se ne bi trebali prikupljati nepotrebni osobni podaci. U tom slučaju, ako bi se drugom vrstom obrade mogao postići isti cilj i ako je ona dostupna u skladu s uvjetima opisanima u scenariju 3.1., nije potrebno upotrebljavati tehnologiju prepoznavanja lica.

75. Kad je riječ o članku 25. OUZP-a, najvažniji element zaštite tehničke i integrirane podataka jest autonomija ispitanika. Konkretno, ispitaniku bi trebalo dati najveći mogući stupanj autonomije da odredi za što će se koristiti njegovi osobni podataci, kao i opsega i uvjeta te uporabe ili obrade[104]. U prvom scenariju ispitanik bi imao autonomiju i kontrolu nad upotrebom, otkrivanjem i brisanjem svojih biometrijskih predložaka, a u drugom scenariju ispitanik bi zadržao određenu kontrolu nad otkrivanjem vlastitog biometrijskog predloška jer bi ključ/lozinka za šifriranje bili pohranjeni kod njega. Međutim, u scenariju 3.1. ispitanik u potpunosti ovisi o izborima voditelja obrade u vezi s obradom svojih biometrijskih podataka te stoga nema izravnu kontrolu nad upotrebom svojeg biometrijskog predloška.

76. Kad je riječ o usklađenosti s člankom 25. OUZP-a, a posebno kako bi se ispunio zahtjev smanjenja količine podataka, obrada predviđena scenarijem 3.1. ne može ispuniti načelo nužnosti. Odbor smatra da se sličan rezultat za ubrzavanje protoka putnika u zračnim lukama može postići na način kojim se manje narušava privatnost. Na primjer, to se može postići bez upotrebe biometrijskih podataka (iako bi korisničko iskustvo u tom slučaju bilo drukčije jer bi moglo biti potrebno dulje vrijeme za predočenje karte za uskrcaj u zrakoplovi, prema potrebi, službenih identifikacijskih isprava). Osim toga, druga rješenja, posebno ona koja se oslanjaju na pohranu biometrijskih podataka u lokalnom novčaniku na uređaju pojedinca ili ona koja zahtijevaju šifriranje podataka određenim ključem pohranjenim na njegovu uređaju, omogućuju postizanje ciljeva na način kojim se manje narušava privatnost.

77. Kad je riječ o načelu proporcionalnosti, obrada predviđena scenarijem 3.1. stvorila bi rizike za prava ispitanika koji se ne bi ublažili predviđenim mjerama s obzirom na suvremena tehnološka dostignuća.

---

[103] Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka, točka 49.

[104] Smjernice EDPB-a 4/2019 o tehničkoj i integriranoj zaštiti podataka, točka 70. U uvodnoj izjavi 7. Opće uredbe o zaštiti podataka dodatno se pojašnjava da bi „[p]ojedinci bi trebali imati nadzor nad vlastitim osobnim podacima".

Čini se da rizik od negativnog učinka na temeljna prava i slobode ispitanika koji bi mogao proizaći iz povrede podataka u središnjoj bazi biometrijskih podataka velikog broja pojedinaca nadmašuje očekivanu korist od obrade, jer je ta korist relativno mala, tj. neznatno jednostavnije i brže provjere. Stoga se njome ne može opravdati visoka razina zadiranja tih mjera u temeljna prava i slobode pojedinaca te obrada predviđena scenarijem 3.1. nije u skladu s načelom proporcionalnosti.

78. S obzirom na navedeno i kao odgovor na pitanje 2.2.1. Odbor zaključuje da, ako se obrada provodi u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama, obrada predviđena scenarijem 3.1.:

- **ne može biti u skladu s člankom 25. OUZP-a**
- **ne bi bila u skladu s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a** ako bi voditelj obrade provodio samo mjere opisane u scenariju 3.1.

3.2.3.2. Scenarij 3.2.: centralizirana pohrana u oblaku, pod kontrolom zračnog prijevoznika

Opis scenarija

79. U scenariju 3.2. upisani biometrijski predložak putnika pohranjen je u oblaku pod kontrolom zračnog prijevoznika ili njegova pružatelja usluga u oblaku (izvršitelj obrade podataka). U Zahtjevu je navedeno da će pružatelj usluga računalstva imati poslovni nastan u EGP-u[105]. U tom su slučaju podaci o putnicima šifrirani, ali se dešifriraju kad se koriste (tj., prilikom uspoređivanja biometrijskih podataka), a ključeve kontrolira zračni prijevoznik ili izvršitelj obrade podataka koji je pružatelja usluga u oblaku. Biometrijski podaci putnika koriste se za identifikaciju putnika (usporedba 1:N), pri čemu N može biti najviše ukupni broj klijenata zračnog prijevoznika[106].

80. Slično prvom i drugom scenariju te scenariju 3.1. i u ovom se slučaju putnici prvo moraju upisati. Međutim, u scenariju 3.2. upis putnika obavlja se jednom i čuva se sve dok putnik ima račun kod aviokompanije. Upis se obavlja na daljinu na odgovarajućoj razini provjere identiteta (npr. odgovarajuća razina osiguranja eIDAS-a) ili na terminalima zračnih luka. Osim toga, uspoređivanje biometrijskih podataka provodi se samo kad se putnici pojave na unaprijed definiranim kontrolnim točkama u zračnoj luci, ali se sama obrada podataka obavlja u oblaku.

81. U zračnoj luci putnici prolaze kroz posebne kontrolne samoposlužne uređaje s kamerom. Biometrijski podaci putnika šalju se putem zahtjeva zračnom prijevozniku na poslužitelj u oblaku, gdje se ti podaci uspoređuju sa središnjom bazom podataka. Putnik se stoga može identificirati i provjeriti je li doista registriran za odlazni let (ili ukrcaj u slučaju kontrole pri ukrcaju).

82. Potencijalno, utvrđene podudarnosti mogu se staviti na raspolaganje većem broju upravitelja zračnih luka ako zračni prijevoznik ima posebni terminal ili pristup zajedničkoj infrastrukturi informacijskog sustava zračne luke. Ovisno o kontrolnoj točki, podaci koji se šalju natrag voditelju obrade kontrolne točke koji podnosi zahtjev mogu se, prema potrebi, svesti na najmanju moguću mjeru, na primjer „da/ne odgovor" ili samu utvrđenu podudarnost. U tom se slučaju voditelju obrade na kontrolnoj točki prenosi samo rezultat zahtjeva i on koristi samo njega.

83. Razdoblje pohrane predloška određuje zračni prijevoznik i može trajati sve dok putnik ima račun kod zračnog prijevoznika.

Procjena EDPB-a

84. Stavovi Odbor o scenariju 3.1.[107] vrijede i za ovaj scenarij.

85. Kad je riječ o načelu i zahtjevima u pogledu sigurnosti (članak 5. stavak 1. točka (f) i članak 32. OUZP-a), obrada iz scenarija 3.2. provodi se u oblaku te bi više subjekata moglo imati pristup takvim podacima, uključujući moguće pružatelje s poslovnim nastanom izvan EGP-a, čak i ako se podaci čuvaju

[105] Francusko nadzorno tijelo pojasnilo je da je to ilustrativan primjer i da bi se mogli predvidjeti i pružatelji usluga računalstva u oblaku koji nema poslovni nastan u EGP-u. Osim toga, mogla bi se razmotriti i druga rješenja za pohranu (npr. bez upotrebe oblaka).
[106] Francusko nadzorno tijelo pojasnilo je da je to ilustrativan primjer i da postoji rješenje prema kojem se biometrijski podaci šalju svaki put prije leta.
[107] Točke od 68. do 77.

u EGP-u[108]. Takva arhitektura podrazumijeva potencijalne rizike u vezi s prijenosom osobnih podataka u treće zemlje. Osim toga, iako su podaci o putnicima šifrirani, dešifriraju se kad se koriste (tj. prilikom uspoređivanja biometrijskih podataka), dok ključeve kontrolira zračni prijevoznik ili izvršitelj obrade podataka koji je pružatelja usluga u oblaku Takva pohrana može dodatno povećati sigurnosni rizik.

86. Stoga su kad je riječ o usklađenosti s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a, mjere predviđene u scenariju 3.2.[109], uzimajući u obzir suvremena tehnološka dostignuća nedovoljne za osiguranje razine sigurnosti primjerene riziku. Na temelju toga, obrada u okviru scenarija 3.2. ne bi bila usklađena s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a ako bi voditelj obrade koristio samo te mjere.

87. Osim toga, prema scenariju 3.2.[110] podaci bi se mogli pohranjivati tijekom duljeg razdoblja (tj. potencijalno dok god ispitanik ima račun kod zračnog prijevoznika). Takvo trajanje pohrane izlaže podatke većem riziku od povrede njihove povjerljivosti i cjelovitosti te se čini da prelazi ono što je strogo nužno i proporcionalno za potrebe obrade. Odbor napominje da razdoblje pohrane podataka nije samo po sebi odlučujući čimbenik za ukupnu usklađenost navedene arhitekture s OUZP-om jer ih voditelji obrade podataka mogu izmijeniti. Međutim, na temelju informacija dostupnih Odboru i sadržanih u opisu scenarija 3.2. nema dovoljno opravdanja za to dugo razdoblje pohrane ni očitih mjera za ublažavanje rizika za pojedince. Na temelju toga, predloženo razdoblje pohrane ne bi bilo ograničeno na ono što je nužno, u skladu s načelom ograničenja pohrane iz članka 5. stavka 1. točke (e) OUZP-a.

88. U svakom slučaju, mjere predložene u scenariju 3.2. ne mogu ispuniti zahtjeve tehničke zaštite podataka iz članka 25. Opće uredbe o zaštiti podataka. U scenariju 3.2. biometrijski predlošci putnika pohranjeni su u oblaku pod kontrolom zračnog prijevoznika ili njegova pružatelja usluga u oblaku (izvršitelj obrade podataka). Kako je prethodno opisano, više subjekata moglo bi imati pristup tim podacima. Nadalje, biometrijski podaci putnika koriste se za identifikaciju putnika (usporedba 1:N), pri čemu N može biti najviše ukupni broj klijenata zračnog prijevoznika. Takva metoda podrazumijeva pronalaženje osobe među skupinom pojedinaca u središnjoj bazi podataka, pri čemu se svako snimljeno lice obrađuje kako bi se provjerilo podudara li se s osobom koja je poznata sustavu. Za razliku od scenarija 3.1, u scenariju 3.2 usporedba bi se mogla provesti u mnogo većem opsegu jer je ovdje kriterij ukupni broj klijenata zračnog prijevoznika, dok je scenarij 3.1 uključivao samo očekivani broj putnika u roku od nekoliko dana.

89. Osim toga, kad je riječ o usklađenosti s člankom 25. OUZP-a, a posebno kako bi se ispunio zahtjev smanjenja količine podataka, obrada predviđena scenarijem 3.2. ne može ispuniti načelo nužnosti. Odbor smatra da bi se sličan rezultat za ubrzavanje protoka putnika u zračnim lukama mogao postići drugim manje nametljivim mjerama, na primjer bez upotrebe biometrijskih podataka, iako bi korisničko iskustvo u tom slučaju bilo drukčije jer bi pokazivanje identifikacijske isprave i karte za ukrcaj u zrakoplov moglo dulje trajati. Osim toga, druga rješenja, posebno ona koja se oslanjaju na pohranu biometrijskih podataka u lokalnom novčaniku na uređaju pojedinca ili ona koja zahtijevaju šifriranje

[108] Mjere za koordinirano izvršenje EDPB-a iz 2022. o upotrebi usluga u oblaku u javnom sektoru, 17. siječnja 2023., str. 19.
[109] Vidjeti točke od 79. do 83.
[110] Vidjeti prethodnu točku 83.

podataka određenim ključem pohranjenim na njegovu uređaju, omogućuju voditelju obrade da postigne cilj na način kojim se manje narušava privatnost.

90. Kad je riječ o načelu proporcionalnosti, obrada predviđena scenarijem 3.2. stvorila bi rizike za prava ispitanika koje se ne bi ublažile predviđenim zaštitnim mjerama. Čini se da negativan učinak na temeljna prava i slobode ispitanika koji bi bio posljedica povrede podataka u središnjoj bazi biometrijskih podataka velikog broja pojedinaca pohranjenih u oblaku nadmašuje očekivanu korist od obrade, budući da je ta korist relativno mala, tj. neznatno jednostavnije i brže provjere. Stoga ta korist ne može opravdati visoku razinu zadiranja tih mjera u temeljna prava i slobode pojedinaca te obrada predviđena scenarijem 3.2. ne može se smatrati proporcionalnom.

91. S obzirom na navedeno i kao odgovor na pitanje 2.3.1. Odbor zaključuje da, ako se obrada provodi u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama, obrada predviđena scenarijem 3.2.:

- **ne može biti u skladu s člankom 25. OUZP-a**
- **ne bi bila u skladu s člankom 5. stavkom 1. točkom (f) i člankom 32. OUZP-a** ako bi voditelj obrade provodio samo mjere opisane u scenariju 3.2.
- **ne bi bila u skladu s člankom 5. stavkom 1. točkom (e) Opće uredbe o zaštiti podataka** jer na temelju informacija dostupnih Odboru ne postoji dostatno opravdanje za razdoblje pohrane predviđeno u scenariju 3.2. Kako bi se poštovalo načelo ograničenja pohrane iz članka 5. stavka 1. točke (e) Opće uredbe o zaštiti podataka, voditelj obrade trebao bi dokazati da se osobni podaci ne pohranjuju dulje nego što je potrebno za svrhe u koje se obrađuju.

4. ZAKLJUČCI

92. Kad je riječ o pitanju 1.1., Odbor na temelju zahtjeva za mišljenje francuskog nadzornog tijela u vezi sa zahtjevima iz članka 5. stavka 1. točke (f), članaka 25. i 32. OUZP-a i na temelju prethodne analize zaključuje sljedeće:

93. upotreba tehnologije prepoznavanja lica za autentifikaciju na temelju biometrijskih podataka u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama (zaštitne kontrolne točke, predaja prtljage, ukrcaj i pristup salonu za putnike) mogla bi se smatrati načelno usklađenom s načelima cjelovitosti i povjerljivosti iz članka 5. stavka 1. točke (f), članaka 25. i 32. OUZP-a, u slučaju arhitekture pohrane, u kojoj je upisani biometrijski predložak svakog putnika pohranjen lokalno na njegovu osobnom uređaju nad kojim samo on ima kontrolu, ako se na nju primjenjuju odgovarajuće zaštitne mjere kako je opisano u točki 46.

94. Kad je riječ o pitanju 2.1.1., Odbor na temelju zahtjeva za mišljenje francuskog nadzornog tijela u vezi sa zahtjevima iz članka 5. stavka 1. točaka (e) i (f) te članaka 25. i 32. OUZP-a i na temelju prethodne analize zaključuje sljedeće:

95. upotreba tehnologije prepoznavanja lica za autentifikaciju na temelju biometrijskih podataka u posebnu svrhu ubrzavanja protoka putnika u zračnim lukama (zaštitne kontrolne točke, predaja prtljage, ukrcaj i pristup salonu za putnike) mogla bi se smatrati načelno usklađenom s načelom ograničenja pohrane iz članka 5. stavka 1. točke (e) i načelima cjelovitosti i povjerljivosti iz članka 5. stavka 1. točke (f) te članaka 25. i 32. OUZP-a u slučaju arhitekture centralizirane pohrane, u kojoj je upisani biometrijski predložak svakog putnika pohranjen u središnjoj bazi podataka u zračnoj luci, pod

kontrolom upravitelja zračne luke, u šifriranom obliku, s ključem/lozinkom koju posjeduje samo pojedinac, ako se na nju primjenjuju odgovarajuće zaštitne mjere kako je opisano u točki 60.

96. Kad je riječ o pitanju 2.2.1., Odbor na temelju zahtjeva za mišljenje francuskog nadzornog tijela u vezi sa zahtjevima iz članka 5. stavka 1. točaka (e) i (f) te članaka 25. i 32. OUZP-a i na temelju prethodne analize zaključuje sljedeće:

97. upotreba tehnologije prepoznavanja lica za identifikaciju na temelju biometrijskih podataka, koja se koristi za ubrzavanje protoka putnika u zračnim lukama (zaštitne kontrolne točke, predaja prtljage, ukrcaj i pristup salonu za putnike) u slučaju arhitekture centralizirane pohrane, kad biometrijski predlošci putnika nisu šifrirani ključem/lozinkom koju posjeduje samo putnik i pohranjeni su u bazi podataka u zračnoj luci (pod kontrolom upravitelja zračne luke), ne može biti u skladu s člankom 25. OUZP-a. Osim toga, takva obrada ne bi bila u skladu s načelom cjelovitosti i povjerljivosti iz članka 5. stavka 1. točke (f) i članka 32. OUZP-a ako bi voditelj obrade koristio samo mjere opisane u scenariju 3.1.

98. Kad je riječ o pitanju 2.3.1., Odbor na temelju zahtjeva za mišljenje francuskog nadzornog tijela u vezi sa zahtjevima iz članka 5. stavka 1. točaka (e) i (f) te članaka 25. i 32. OUZP-a i na temelju prethodne analize zaključuje sljedeće:

99. upotreba tehnologije prepoznavanja lica za identifikaciju na temelju biometrijskih podataka, koja se koristi za ubrzavanje protoka putnika u zračnim lukama (zaštitne kontrolne točke, predaja prtljage, ukrcaj i pristup salonu za putnike) u slučaju arhitekture centralizirane pohrane, kad biometrijski predlošci putnika nisu šifrirani ključem/lozinkom koju posjeduje samo putnik i pohranjeni su u oblaku (pod kontrolom upravitelja zračnog prijevoznika), ne može biti u skladu s člankom 25. OUZP-a. Osim toga, takva obrada ne bi bila u skladu s načelom cjelovitosti i povjerljivosti iz članka 5. stavka 1. točke (f) i članka 32. OUZP-a ako bi voditelj obrade koristio samo mjere opisane u scenariju 3.2. Naposljetku, na temelju opisa scenarija 3.2. i informacija dostupnih Odboru, obrada ne bi bila u skladu s načelom ograničenja pohrane iz članka 5. stavka 1. točke (e) OUZP-a.

Za Europski odbor za zaštitu podataka

Predsjednica

(Anu Talus)