Avizul Comitetului (Articolul 64)

Avizul nr. 11/2024 privind utilizarea recunoașterii faciale pentru eficientizarea fluxului de pasageri în aeroporturi [compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD]

Versiunea 1.1

Adoptat la 23 mai 2024

Versiunea 1.1	28 mai 2024	Corecție gramaticală în rezumat (paginile 3 și 4) și la punctele 77 și 90 din aviz
Versiunea 1.0	23 mai 2024	Adoptarea avizului

Rezumat

Autoritatea de supraveghere franceză a solicitat Comitetului european pentru protecția datelor să emită un aviz privind utilizarea tehnologiei de recunoaștere facială de către operatorii aeroportuari și companiile aeriene în scopul autentificării sau identificării bazate pe date biometrice a pasagerilor în vederea eficientizării fluxului de pasageri în aeroporturi.

Ca observație preliminară, Comitetul reamintește că utilizarea datelor biometrice și, în special, a tehnologiei de recunoaștere facială implică riscuri sporite pentru drepturile și libertățile persoanelor vizate. Aceasta implică prelucrarea datelor biometrice care beneficiază de o protecție specială în temeiul articolului 9 din RGPD. Înainte de a utiliza astfel de tehnologii, chiar dacă acestea ar fi considerate deosebit de eficace, operatorii ar trebui să evalueze impactul asupra drepturilor și libertăților fundamentale ale persoanelor vizate și să analizeze dacă scopul legitim al prelucrării poate fi atins prin mijloace mai puțin intruzive.

Domeniul de aplicare al prezentului aviz, astfel cum reiese din cerere, este limitat la compatibilitatea prelucrării cu **articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD** în **scopul specific de a eficientiza fluxul de pasageri în aeroporturi** la patru puncte de control specifice, și anume la punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri. Prezentul aviz nu include o analiză deplină și completă a respectării RGPD de către operatorul (operatorii) relevant (relevanți) în fiecare caz, precum și de către persoana (persoanele) împuternicită (împuternicite) de acesta (aceștia), dacă este cazul. Prin urmare, prezentul aviz nu aduce atingere unei analize juridice și tehnice de la caz la caz, bazată pe prelucrarea și circumstanțele specifice avute în vedere de operator. În plus, analiza temeiului juridic aplicabil nu intră în sfera întrebărilor adresate Comitetului în cerere și, prin urmare, valabilitatea consimțământului pentru o astfel de prelucrare, în conformitate cu articolele 6, 7 și 9 din RGPD, nu este examinată în prezentul aviz. De asemenea, prezentul aviz nu aduce atingere restricțiilor privind utilizarea datelor biometrice în temeiul dreptului intern al statelor membre.

În prezentul aviz, Comitetul evaluează conformitatea prelucrării cu dispozițiile RGPD menționate mai sus în contextul a **patru scenarii specifice**.

Primul scenariu implică stocarea unui model biometric înregistrat în posesia persoanei, de exemplu, pe dispozitivul personal, sub controlul exclusiv al acesteia, în vederea autentificării pasagerului (comparație 1:1) atunci când acesta trece prin punctele de control din aeroport menționate mai sus.

Comitetul concluzionează că s-ar putea considera că măsurile alese respectă principiul necesității dacă operatorul poate demonstra că nu există soluții alternative mai puțin intruzive care ar permite atingerea aceluiași obiectiv într-un mod la fel de eficace. În plus, caracterul intruziv al prelucrării poate fi contrabalansat de implicarea activă a pasagerilor, având în vedere că modelul lor biometric este stocat exclusiv în posesia acestora, de exemplu, pe dispozitivul personal, sub controlul exclusiv al acestora, iar datele lor sunt șterse la scurt timp după finalizarea punerii în corespondență. Pe această bază, Comitetul concluzionează că prelucrarea avută în vedere în primul scenariu **ar putea fi considerată, în principiu, compatibilă cu articolul 5 alineatul (1) litera (f) și cu articolele 25 și 32 din RGPD**, sub rezerva punerii în aplicare a unor garanții adecvate.

Comitetul a identificat garanțiile minime care ar trebui puse în aplicare în cazul unei soluții similare cu primul scenariu.

Al doilea scenariu implică stocarea centralizată, în cadrul aeroportului, a unui model biometric înregistrat într-o formă criptată, cu o cheie/metodă secretă aflată exclusiv în posesia pasagerului respectiv. Acest lucru permite autentificarea pasagerului (comparație 1:1) pe măsură ce acesta trece prin punctele de control din aeroport menționate mai sus. Înregistrarea este valabilă pentru o anumită perioadă, de exemplu, un an de la data efectuării ultimului zbor și până la data expirării pașaportului.

Comitetul concluzionează că s-ar putea considera că prelucrarea respectă principiul necesității dacă operatorul poate demonstra că nu există soluții alternative mai puțin intruzive care ar permite atingerea aceluiași obiectiv într-un mod la fel de eficace. În plus, caracterul intruziv al prelucrării poate fi contrabalansat de implicarea activă a pasagerului, cheia/metoda secretă asociată datelor sale biometrice criptate fiind sub controlul exclusiv al acestuia. Presupunând că operatorul pune în aplicare garanții adecvate, riscurile de securitate generate de utilizarea unei baze de date centralizate în acest scenariu ar putea fi atenuate, iar impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate ar putea fi considerat proporțional cu beneficiul anticipat. În ceea ce privește principiul limitării legate de stocare, nu a fost furnizată Comitetului nicio informație care să justifice perioada lungă de stocare. Pentru a asigura compatibilitatea cu articolul 5 alineatul (1) litera (e) din RGPD în acest scenariu, operatorii ar trebui să poată justifica de ce perioada de păstrare avută în vedere este necesară pentru îndeplinirea scopului prelucrării în cazuri specifice. Comitetul recomandă operatorilor să aibă în vedere cea mai scurtă perioadă de stocare posibilă, oferind totodată pasagerilor opțiunea de a-și alege perioada de stocare preferată. Pe această bază, Comitetul concluzionează că prelucrarea avută în vedere în scenariul 2 **ar putea fi considerată, în principiu, compatibilă cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD,** sub rezerva punerii în aplicare a unor garanții adecvate.

Comitetul a identificat garanțiile minime care ar trebui puse în aplicare în cazul unei soluții similare cu cel de al doilea scenariu.

Al treilea scenariu implică stocarea centralizată, în cadrul aeroportului, a unui model biometric înregistrat într-o formă criptată, sub controlul operatorului aeroportuar. Acest lucru permite identificarea pasagerului (comparație 1:N), pe măsură ce acesta trece prin punctele de control din aeroport menționate mai sus. Perioada de stocare în acest scenariu este, de regulă, de 48 de ore, iar datele sunt șterse după decolarea avionului.

Întrucât datele de identificare și cele biometrice sunt stocate într-o bază de date centrală, compromiterea confidențialității acesteia poate genera ulterior riscul accesării întregului set de date și ar putea permite identificarea neautorizată sau ilegală a pasagerilor în alte medii. Stocarea centralizată sub controlul operatorului aeroportuar implică, de asemenea, pierderea într-o mai mare măsură de către pasager a controlului asupra datelor sale. Comitetul consideră că un efect similar în ceea ce privește eficientizarea fluxului de pasageri în aeroporturi poate fi obținut într-un mod mai puțin intruziv, iar impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate care ar rezulta din încălcarea securității datelor biometrice stocate într-o bază de date centralizată pare să depășească beneficiul anticipat al prelucrării. Prin urmare, prelucrarea nu respectă principiul necesității și al proporționalității. Pe această bază, Comitetul concluzionează că prelucrarea avută în vedere în al treilea scenariu **nu poate fi compatibilă cu articolul 25 din RGPD**. În plus, prelucrarea **nu ar respecta nici articolul 5 alineatul (1) litera (f) și nici articolul 32 din RGPD** dacă un operator s-ar limita la măsurile descrise în acest scenariu.

Al patrulea scenariu implică stocarea centralizată a unui model biometric înregistrat într-o formă criptată în cloud, sub controlul companiei aeriene sau al furnizorului de servicii de cloud al acesteia. Acest lucru permite identificarea pasagerului (comparație 1:N) pe măsură ce acesta trece prin

punctele de control din aeroport menționate mai sus. Perioada de stocare în acest scenariu poate fi echivalentă cu perioada în care clientul deține un cont la compania aeriană.

Întrucât datele de identificare și cele biometrice sunt stocate într-o bază de date centrală în cloud, mai multe entități ar putea avea acces la aceste date, inclusiv, eventual, furnizori din afara SEE. Datele pasagerului sunt decriptate atunci când sunt utilizate, iar cheile se află sub controlul companiei aeriene sau al persoanelor împuternicite de aceasta, putând astfel crește riscurile de încălcare a securității datelor. Stocarea centralizată implică, de asemenea, pierderea într-o mai mare măsură de către pasager a controlului asupra datelor sale. În plus, datele ar putea fi stocate pentru o perioadă mare de timp, fapt care crește riscurile de încălcare a securității acestora și pare să depășească ceea ce este strict necesar și proporțional în scopul prelucrării, cu excepția cazului în care se iau măsuri suplimentare clare pentru a atenua riscurile pentru pasageri.

Comitetul consideră că un efect similar în ceea ce privește eficientizarea fluxului de pasageri în aeroporturi poate fi obținut într-un mod mai puțin intruziv, iar impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate care ar putea rezulta din încălcarea securității datelor biometrice stocate într-o bază de date centralizată pare să depășească beneficiul anticipat al prelucrării. Prin urmare, prelucrarea nu respectă principiul necesității și al proporționalității. Pe această bază, Comitetul concluzionează că prelucrarea avută în vedere în al patrulea scenariu **nu poate fi compatibilă cu articolul 25 din RGPD**. În plus, prelucrarea **nu ar respecta articolul 5 alineatul (1) litera (e) din RGPD** pe baza informațiilor de care dispune Comitetul și **nici articolul 5 alineatul (1) litera (f) și articolul 32 din RGPD** dacă un operator s-ar limita la măsurile descrise în acest scenariu.

Cuprins

Comitetul european pentru protecția datelor

Având în vedere articolul 63 și articolul 64 alineatul (2) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „**RGPD**”),

Având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

Având în vedere articolele 10 și 22 din Regulamentul de procedură (denumit în continuare „**RP al CEPD**”) al Comitetului european pentru protecția datelor (denumit în continuare „**Comitetul**” sau „**CEPD**”),

Întrucât:

(1) Principalul rol al Comitetului este acela de a asigura aplicarea coerentă a RGPD în întregul Spațiu Economic European (denumit în continuare „**SEE**”). Articolul 64 alineatul (2) din RGPD prevede că orice autoritate de supraveghere (denumită în continuare „**AS**”), președintele Comitetului sau Comisia Europeană poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru al SEE să fie examinată de Comitet în vederea obținerii unui aviz.

(2) Avizul Comitetului este adoptat în temeiul articolului 64 alineatul (3) din RGPD, coroborat cu articolul 10 alineatul (2) din RP al CEPD, în termen de opt săptămâni de la data la care președintele și autoritatea de supraveghere competentă au declarat dosarul complet. Prin decizia președintelui, această perioadă poate fi prelungită cu șase săptămâni, în funcție de complexitatea chestiunii.

adoptă prezentul aviz:

1 INTRODUCERE

1.1 Rezumatul situației de fapt

1. La 16 februarie 2024, autoritatea de supraveghere franceză (denumită în continuare „**AS FR**”) a solicitat Comitetului să emită un aviz privind compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD a utilizării tehnologiei de recunoaștere facială de către operatorii aeroportuari și companiile aeriene în scopul autentificării sau identificării bazate pe date biometrice a pasagerilor[2], în vederea eficientizării fluxului de pasageri la punctele de control de securitate din

[1] Trimiterile la „**statele membre**” din acest aviz trebuie înțelese ca trimiteri la „statele membre ale SEE”. Trimiterile la „Uniune” sau la „UE” din acest aviz trebuie înțelese ca trimiteri la „SEE”.

[2] În contextul prezentului aviz, „**pasager**” se referă la o persoană vizată ale cărei date cu caracter personal sunt prelucrate în scopul specific descris în aviz. În continuare, în prezentul aviz, termenii „pasager” și „persoană” sunt utilizați în mod interschimbabil.

aeroport[3], de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri (cu excepția controalelor la frontieră și a verificărilor efectuate de magazinele scutite de taxe vamale) (denumită în continuare „**cererea**"). AS FR a anexat la cererea sa o descriere a cazurilor tipice de utilizare (anexa I).

2. În cererea sa, AS FR observă că modelele testate în prezent în mai multe aeroporturi din UE variază de la un stat membru la altul, generând posibile divergențe de interpretare între autoritățile de supraveghere și un risc de producere a unor efecte diferite asupra drepturilor și libertăților fundamentale ale persoanelor vizate din UE[4].

3. Comitetul consideră că, pentru a oferi un răspuns la cerere, trebuie să se răspundă la următoarele întrebări:

4. **Întrebarea 1**:

1.1. Poate utilizarea tehnologiei de recunoaștere facială pentru autentificarea bazată pe date biometrice **cu scopul specific de a eficientiza fluxul de pasageri în aeroporturi** (punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri) să fie compatibilă cu **articolul 5 alineatul (1) litera (f) și cu articolele 25 și 32 din RGPD** în cazul unei arhitecturi de stocare în care modelul biometric al fiecărui pasager este stocat **exclusiv în posesia acestuia**, de exemplu, local, pe dispozitivul personal, sub controlul exclusiv al acestuia?

1.2. În cazul în care o astfel de prelucrare ar fi considerată compatibilă cu dispozițiile menționate mai sus, ce garanții minime adecvate ar fi necesare, în lumina articolelor 25 și 32 din RGPD?

Întrebarea 2:

2.1. Poate utilizarea tehnologiei de recunoaștere facială pentru identificarea bazată pe date biometrice **cu scopul specific de a eficientiza fluxul de pasageri în aeroporturi** (punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri) să fie compatibilă cu **articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD** în cazul unei arhitecturi de stocare **centralizată** în care modelul biometric al fiecărui pasager este stocat într-o bază de date centrală:

2.1.1. Într-o bază de date centrală din cadrul aeroportului, sub controlul operatorului aeroportuar, într-o formă criptată, cu o cheie/metodă secretă aflată exclusiv în posesia persoanei respective (de exemplu, pe telefonul său mobil), pentru autentificare?

2.1.2. În cazul în care o astfel de prelucrare ar fi considerată compatibilă, ce garanții minime adecvate ar fi necesare, în lumina articolelor 25 și 32 din RGPD?

2.2.1. Într-o bază de date centrală din cadrul aeroportului, sub controlul operatorului aeroportuar, într-o formă criptată, cu chei deținute de operatorul aeroportuar, pentru identificare?

[3] În sensul prezentului aviz, „**punctele de control de securitate din aeroport**" se referă la controalele de securitate realizate sub responsabilitatea operatorului aeroportuar pe care pasagerii trebuie să le efectueze pentru a trece din terminalul de plecări în zona de îmbarcare sau la poarta de îmbarcare.
[4] Cererea, p. 1.

2.2.2. În cazul în care o astfel de prelucrare ar fi considerată compatibilă, ce garanții minime adecvate ar fi necesare, în lumina articolelor 25 și 32 din RGPD?

2.3.1. În cloud, sub controlul companiei aeriene sau al furnizorului său de servicii (persoană împuternicită de operator), într-o formă criptată, cu chei deținute de compania aeriană sau de furnizorul său de servicii, pentru identificare?

2.3.2. În cazul în care o astfel de prelucrare ar fi considerată compatibilă, ce garanții minime adecvate ar fi necesare, în lumina articolelor 25 și 32 din RGPD?

5. După ce AS FR a declarat dosarul complet la 16 februarie 2024, iar președintele Comitetului a făcut același lucru la 23 februarie 2024, dosarul a fost difuzat de secretariat la 23 februarie 2024. Președintele Ccomitetului a decis, în conformitate cu articolul 64 alineatul (3) din RGPD coroborat cu articolul 10 alineatul (2) din RP al CEPD, să prelungească termenul implicit de opt săptămâni cu încă șase săptămâni, având în vedere complexitatea chestiunii.

1.2 Admisibilitatea cererii de aviz în temeiul articolului 64 alineatul (2) din RGPD

6. Articolul 64 alineatul (2) din RGPD prevede că orice autoritate de supraveghere poate solicita ca orice chestiune de aplicare generală sau care produce efecte în mai mult de un stat membru să fie examinată de Comitet în vederea obținerii unui aviz.

7. Comitetul consideră că cererea AS FR privind compatibilitatea utilizării tehnologiei de recunoaștere facială pentru autentificarea sau identificarea bazată pe date biometrice cu scopul specific de eficientizare a fluxului de pasageri în aeroporturi se referă la chestiuni „care produc efecte în mai mult de un stat membru”, întrucât, astfel cum se explică în cerere[5], în prezent sunt în curs de implementare mai multe proiecte în aeroporturile statelor membre și se estimează că o astfel de utilizare va crește în următorii ani. Modelele testate în prezent de diferite aeroporturi și companii aeriene variază semnificativ de la un stat membru la altul, generând astfel riscul ca, din perspectiva protecției datelor, să se producă efecte divergente în mai mult de un stat membru.

8. De asemenea, Comitetul consideră că cererea AS FR are consecințe importante în ceea ce privește aplicarea principiilor prevăzute la articolul 5 alineatul (1) literele (e) și (f) din RGPD și cerințele aplicabile operatorilor în temeiul articolului 25 din RGPD, precum și cerințele aplicabile operatorilor și persoanelor împuternicite de operatori în temeiul articolului 32 din RGPD. Prin urmare, această cerere se referă la o „chestiune de aplicare generală” în sensul articolului 64 alineatul (2) din RGPD, întrucât se referă la interpretarea consecventă a principiului limitării legate de stocare [articolul 5 alineatul (1) litera (e) din RGPD] și a principiului integrității și confidențialității [articolul 5 alineatul (1) litera (f) din RGPD], precum și a noțiunilor de protecție a datelor începând cu momentul conceperii și în mod implicit (articolul 25 din RGPD) și de securitate a datelor (articolul 32 din RGPD) pentru a asigura, printre altele, aplicarea coerentă a acestor dispoziții în SEE.

[5] Cererea, p. 3.

9. Orice posibile poziții divergente între statele membre cu privire la interpretarea articolului 5 alineatul (1) literele (e) și (f) și a articolelor 25 și 32 din RGPD ar crește riscul ca operatorii aeroportuari și companiile aeriene să dezvolte proiecte de recunoaștere facială într-un mod inconsecvent. Întrucât AS FR a demonstrat necesitatea clară a unei interpretări consecvente a acestor dispoziții în ceea ce privește tehnologia de recunoaștere facială pentru autentificarea sau identificarea bazată pe date biometrice a pasagerilor în vederea eficientizării fluxul de pasageri în aeroporturi[6], Comitetul consideră că cererea este justificată, în conformitate cu articolul 10 alineatul (3) din RP al CEPD.

10. În conformitate cu articolul 64 alineatul (3) din RGPD, CEPD nu emite un alt aviz dacă a emis deja un aviz cu privire la aceeași chestiune[7]. CEPD nu a oferit încă răspunsuri la întrebările care decurg din cerere. Deși Ghidul nr. 3/2019 al CEPD privind mijloacele video[8] include deja unele elemente utile privind măsurile de securitate care ar trebui aplicate prelucrării datelor biometrice, acesta nu abordează toate aspectele legate de întrebările care decurg din cerere. În plus, ghidurile disponibile ale CEPD, inclusiv Ghidul nr. 3/2019 al CEPD privind mijloacele video, nu includ orientări specifice cu privire la posibilele elemente care trebuie verificate în legătură cu stocarea centralizată sau descentralizată a datelor biometrice pentru identificarea sau autentificarea pasagerilor în vederea eficientizării fluxului de pasageri în aeroporturi și cu privire la compatibilitatea unei astfel de prelucrări cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD.

11. Din aceste motive, Comitetul consideră că cererea este admisibilă și că întrebările care decurg din aceasta ar trebui analizate într-un aviz adoptat în temeiul articolului 64 alineatul (2) din RGPD.

2 DOMENIUL DE APLICARE ȘI CONTEXTUL AVIZULUI

2.1 Domeniul de aplicare al avizului

12. Prezentul aviz se referă numai la compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD a utilizării tehnologiei de recunoaștere facială pentru autentificarea sau identificarea bazată pe date biometrice a pasagerilor de către operatorii aeroportuari și companiile aeriene, **în scopul specific de a eficientiza fluxul de pasageri în aeroporturi**, mai precis la punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri, conform cererii.

13. În ceea ce privește **domeniul de aplicare al prezentului aviz**, Comitetul clarifică următoarele aspecte:

1) Prelucrarea datelor cu caracter personal în cadrul controalelor la frontieră și al verificărilor efectuate de magazinele scutite de taxe nu intră în domeniul de aplicare al prezentului aviz, întrucât aceasta este efectuată de alți operatori decât operatorii aeroportuari și companiile aeriene.

2) Utilizarea tehnologiei de recunoaștere facială, chiar dacă se bazează pe scenariile descrise mai jos în secțiunea 3.2, în alte scopuri (cum ar fi asigurarea respectării legii)

[6] Cererea, p. 1-3.
[7] Articolul 64 alineatul (3) din RGPD și articolul 10 alineatul (4) din Regulamentul de procedură al CEPD.
[8] Ghidul 3/2019 al CEPD privind prelucrarea datelor cu caracter personal prin mijloace video, versiunea 2.0, adoptat la 29 ianuarie 2020 (denumit în continuare „**Ghidul nr. 3/2019 al CEPD privind mijloacele video**”).

sau de către alte părți, chiar dacă în scopuri similare, nu intră în domeniul de aplicare al prezentului aviz.

3) Prezentul aviz examinează doar prelucrarea datelor cu caracter personal ale pasagerilor și nu se referă la alte tipuri de persoane vizate, cum ar fi personalul operatorilor aeroportuari sau al companiilor aeriene.

4) Prezentul aviz examinează cererea, astfel cum a fost prezentată de AS FR, în ceea ce privește compatibilitatea arhitecturilor de stocare a modelelor biometrice ale pasagerilor cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD. În această privință, prezentul aviz nu include o analiză deplină și completă a respectării RGPD de către operatorul (operatorii) relevant (relevanți) în fiecare caz, precum și de către persoana (persoanele) împuternicită (împuternicite) de acesta (aceștia), dacă este cazul. Acest lucru este deosebit de important având în vedere că aceste tehnologii implică riscuri sporite asociate cu prelucrarea categoriilor speciale de date în conformitate cu articolul 9 din RGPD. Prin urmare, prezentul aviz nu aduce atingere unei evaluări referitoare la alte dispoziții ale RGPD în ceea ce privește utilizarea tehnologiilor de recunoaștere facială, inclusiv în sectorul specific vizat de cerere sau unei analize juridice și tehnice de la caz la caz, bazată pe prelucrarea și circumstanțele specifice avute în vedere de operator.

5) Prezentul aviz nu examinează prelucrarea datelor cu caracter personal ale copiilor și nu aduce atingere niciunei cerințe specifice aplicabile în acest sens.

6) Prezentul aviz nu aduce atingere cerințelor legale și restricțiilor suplimentare privind utilizarea datelor biometrice care decurg din dreptul intern al statelor membre[9].

7) Nicio concluzie din prezentul aviz nu aduce atingere evoluțiilor tehnologice ulterioare.

8) Prezentul aviz examinează patru scenarii, ale căror caracteristici specifice sunt descrise mai jos în secțiunea 3.2. Acesta nu abordează alte scenarii, chiar dacă prelucrarea este efectuată în aceleași scopuri.

14. În cererea sa, AS FR a menționat că prelucrarea datelor biometrice ale pasagerilor în scopul eficientizării fluxului de pasageri în aeroporturi s-ar baza pe ipoteza că aceștia își dau consimțământul pentru o astfel de prelucrare, consimțământ care ar putea constitui temeiul juridic în temeiul RGPD[10]. **Cu toate acestea, analiza <u>temeiului juridic aplicabil nu intră în sfera</u> întrebărilor adresate CEPD în cerere și, prin urmare, <u>valabilitatea consimțământului pentru o astfel de prelucrare, în conformitate cu articolele 6, 7 și 9 din RGPD, nu este examinată în prezentul aviz</u>.**

[9] De exemplu, articolul 9 alineatul (4) din RGPD prevede că statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date biometrice.
[10] Cererea, anexa I.

15. Cu toate acestea, CEPD menționează în termeni generali că, în cazul în care operatorii relevanți s-ar baza pe acest temei juridic, aceștia ar trebui să obțină consimțământul explicit valabil[11] din partea persoanelor care doresc să utilizeze astfel de servicii. Acest consimțământ explicit ar trebui să fie acordat în mod liber, specific și în cunoștință de cauză[12], iar îndeplinirea acestor condiții ar fi analizată de la caz la caz. Aceasta înseamnă, printre altele, că:

    1) Persoanele vizate ar trebui să își poată retrage cu ușurință consimțământul în orice moment și fără a fi prejudiciate[13].

    2) Consimțământul se consideră a fi acordat în mod liber numai atunci când tehnologiile bazate pe date biometrice sunt utilizate voluntar, persoanele vizate având posibilitatea de a alege liber dacă să utilizeze sau nu aceste servicii, fără consecințe negative (cum ar fi întârzieri mult mai mari pentru pasagerii care nu își dau consimțământul[14]) și fără stimulente, costuri sau avantaje suplimentare asociate[15].

    3) De asemenea, ar trebui obținut consimțământul explicit al persoanelor ale căror date biometrice sunt prelucrate, chiar dacă acestea nu au optat pentru a fi identificate sau autentificate prin astfel de mijloace. Cu alte cuvinte, este esențial ca fețele persoanelor care nu și-au exprimat consimțământul explicit pentru recunoașterea facială în scopul preconizat să nu fie scanate de camerele video. Acest lucru poate fi realizat, de exemplu, prin culoare specifice rezervate recunoașterii faciale și prin semnalizarea adecvată și separarea fizică de fluxurile de controale nebiometrice pentru a permite o identificare clară a acestor culoare.

    4) Fără a aduce atingere posibilității de a considera consimțământul drept temei juridic aplicabil pentru o astfel de prelucrare, principiile privind necesitatea și proporționalitatea operațiunilor de prelucrare, consacrate la articolul 5 din RGPD, se aplică în continuare chiar și atunci când persoanele fizice și-au dat consimțământul explicit pentru utilizarea datelor lor biometrice[16].

---

[11] În conformitate cu articolul 4 punctul 14 și cu articolul 9 alineatul (1) din RGPD, precum și cu articolul 9 alineatul (2) litera (a) din RGPD, se interzice prelucrarea de date biometrice pentru identificarea unică a unei persoane fizice, exceptând cazul în care persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede că interdicția prevăzută la articolul 9 alineatul (1) din RGPD să nu poată fi ridicată prin consimțământul persoanei vizate. A se vedea, de asemenea, considerentele 51, 52 și 53 din RGPD.

[12] Articolul 4 punctul 11 și articolul 7 din RGPD.

[13] Articolul 7 alineatul (4) și considerentul 50 din RGPD.

[14] De exemplu, aceasta ar putea include considerații precum conceperea unui sistem pentru a evita crearea unei presiuni sociale asupra pasagerilor care nu doresc să își dea consimțământul, evitând ca alegerea acestuia să aibă un impact negativ asupra altor pasageri.

[15] Orientările nr. 05/2020 ale CEPD privind consimțământul în temeiul Regulamentului 2016/679, versiunea 1.1, adoptate la 4 mai 2020 (denumite în continuare „**Orientările nr. 05/2020 ale CEPD privind consimțământul**"), punctele 46 și 48.

[16] Idem, punctul 5.

16. În cerere se precizează[17] că operatorii aeroportuari ar acționa în calitate de operatori în ceea ce privește prelucrarea la punctele de control de securitate din aeroport, în timp ce companiile aeriene ar acționa în calitate de operatori în ceea ce privește prelucrarea la punctele de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri. Prin urmare, Comitetul remarcă faptul că în prelucrarea descrisă în cerere ar putea fi implicați diferiți actori și că aceasta nu a evaluat aplicarea rolurilor de operator (asociat) și/sau de persoană împuternicită de operator în scenariile descrise mai jos în secțiunea 3.2 din prezentul aviz. Pentru respectarea cerințelor din RGPD, este necesară identificarea în fiecare caz a actorilor implicați și stabilirea clară a responsabilităților acestora[18].

17. În plus, Comitetul precizează că în UE nu există în prezent o cerință legală uniformă pentru operatorii aeroportuari și companiile aeriene de a identifica pasagerii și de a verifica dacă numele de pe cartea de îmbarcare a pasagerilor corespunde numelui din documentul lor de identitate în toate punctele de control menționate mai sus[19]. Astfel, aceste cerințe intră sub incidența legislației naționale, care poate varia de la un stat membru la altul. În unele state membre, o astfel de verificare poate fi necesară pentru unele puncte de control (de exemplu, predarea bagajelor sau îmbarcare), în timp ce în altele nu sunt necesare în prezent astfel de verificări[20]. Existența unor obligații legale de verificare a identității pasagerilor are un impact direct asupra diferitelor practici ale aeroporturilor.

18. Prin urmare, în situațiile **în care nu există obligația verificării identității pasagerilor printr-un document de identitate oficial nu ar trebui efectuată o verificare pe baza datelor biometrice, deoarece acest lucru ar conduce la o prelucrare excesivă a datelor, întrucât implică prelucrarea de date suplimentare în comparație cu situația în cauză și ar depăși ceea ce este necesar în raport cu scopul relevant, încălcând principiul reducerii la minimum a datelor prevăzut la articolul 5 alineatul (1) litera (c) din RGPD.** Acest aspect trebuie luat în considerare la examinarea tuturor scenariilor descrise mai jos în secțiunea 3.2 din prezentul aviz.

2.2 Noțiuni de bază

[17] Cererea, anexa I.

[18] În conformitate cu articolul 4 punctele 7 și 8, articolul 5 alineatul (2) și articolele 24, 26, 28 și 29 din RGPD. A se vedea, de asemenea, Orientările nr. 07/2020 ale CEPD privind conceptele de operator și persoană împuternicită de operator în cadrul RGPD, versiunea 2.1, adoptate la 7 iulie 2021.

[19] Regulamentul relevant la nivelul UE este Regulamentul de punere în aplicare (UE) 2015/1998 al Comisiei din 5 noiembrie 2015 de stabilire a măsurilor detaliate de implementare a standardelor de bază comune în domeniul securității aviației. Acest regulament nu abordează însă verificarea documentelor oficiale de identitate la punctele de control din aeroporturi, iar statele membre au libertatea de a reglementa acest aspect la nivel național.

[20] Ceea ce înseamnă că, în prezent, fie nu se efectuează nicio verificare, fie se verifică numai existența cărții de îmbarcare. De exemplu, pe baza Protocolului din 22 mai 1954 privind scutirea resortisanților Danemarcei, Finlandei, Norvegiei și Suediei de obligația de a deține un pașaport sau un permis de ședere pe durata șederii într-o altă țară scandinavă decât cea de origine, începând cu 1 iulie 1954, cetățenii Norvegiei, Danemarcei, Finlandei și Suediei sunt scutiți de obligația de a deține un pașaport sau un alt tip de document de călătorie atunci când călătoresc între aceste țări.

19. Pentru a se încadra în datele biometrice definite la articolul 4 punctul 14 din RGPD[21], prelucrarea datelor brute, cum ar fi caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, trebuie să implice măsurarea acestor caracteristici, întrucât datele biometrice sunt rezultatul unor astfel de măsurători[22].

20. Prin utilizarea imaginii feței unei persoane (o fotografie sau un material video), numită „**eșantion**" biometric, se poate extrage o reprezentare digitală a caracteristicilor distincte ale feței respective (numită „**model**")[23]. În plus, Comitetul reamintește că „un model biometric este o reprezentare digitală a caracteristicilor unice care au fost extrase dintr-un eșantion biometric și care pot fi stocate într-o bază de date biometrice"[24] care permit sau confirmă identificarea unică a unei persoane fizice. În plus, „se presupune că acest model este unic și specific fiecărei persoane și este, în principiu, permanent în timp"[25]. De regulă, în cadrul unui proces de comparare care vizează identificarea sau autentificarea unei persoane prin recunoaștere facială, un model biometric primit este comparat cu datele stocate fie pentru a verifica o corespondență, fie pentru a găsi o persoană într-o bază de date[26].

21. Tehnologia de recunoaștere facială poate îndeplini două funcții distincte – autentificare[27] și identificare[28]. Deși sunt funcții distincte, ambele se bazează pe prelucrarea datelor biometrice

[21] A se vedea, de asemenea, considerentele 51, 52 și 53 din RGPD.
[22] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 74.
[23] Orientările nr. 5/2022 ale CEPD privind utilizarea tehnologiei de recunoaștere facială în domeniul aplicării legii, versiunea 2.0, adoptate la 26 aprilie 2023 (denumite în continuare „**Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii**"), punctele 7 și 8.
[24] Idem, punctul 9.
[25] Idem.
[26] Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctele 10-11; a se vedea, de asemenea, standardul internațional ISO/IEC 2382-37, 2022-03, disponibil la: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [accesat ultima dată la 23 mai 2024] (denumit în continuare „**ISO/IEC 2382-37**").
[27] Comitetul precizează că viitorul Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul privind inteligența artificială) (nepublicat încă în Jurnalul Oficial) definește, de asemenea, la articolul 3 punctul 36, „verificarea biometrică" ca fiind „verificarea automată, pe baza unei comparații între două seturi de date, inclusiv autentificarea, a identității persoanelor fizice prin compararea datelor biometrice ale acestora cu datele biometrice furnizate anterior" [a se vedea Rezoluția legislativă a Parlamentului European din 13 martie 2024 referitoare la propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) și de modificare a anumitor acte legislative ale Uniunii [COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)].
[28] Idem, articolul 3 punctul 35 din Regulamentul privind inteligența artificială definește „identificarea biometrică" ca fiind „recunoașterea automată a caracteristicilor fizice, fiziologice, comportamentale sau psihologice ale omului în scopul stabilirii identității unei persoane fizice prin compararea datelor biometrice ale persoanei respective cu datele biometrice ale persoanelor stocate într-o bază de date".

referitoare la o persoană fizică identificată sau identificabilă[29] și, prin urmare, constituie o prelucrare de categorii speciale de date cu caracter personal în temeiul articolului 9 din RGPD[30].

22. În special:

> **Autentificarea** are scopul de a verifica, prin comparație, dacă o persoană este cine pretinde că este. Aceasta se numește și verificare unu la unu.
>
> **Identificarea** vizează căutarea într-o bază de date cu modele biometrice înregistrate pentru a găsi identificatori care pot fi atribuiți unei singure persoane. Aceasta se mai numește și identificare realizată prin identificare de tip „unul la mai mulți”.

23. În ambele cazuri (identificare și autentificare), tehnicile de recunoaștere facială se bazează pe o corespondență estimată între modele: cel care este comparat și cel (cele) de referință. Din acest punct de vedere, ele sunt probabilistice: comparația deduce o probabilitate, mai mare sau mai mică, că persoana în cauză este într-adevăr persoana care trebuie autentificată sau identificată; dacă această probabilitate depășește un anumit prag din sistem, definit de utilizator sau de dezvoltatorul sistemului, sistemul va presupune că există o corespondență[31].

[29] ISO/IEC 2382-37.
[30] Articolul 4 punctul 14 din RGPD și Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctul 12.
[31] Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctul 11. A se vedea, de asemenea, ISO/IEC 2382-37.

3 CU PRIVIRE LA TEMEINICIA CERERII

3.1 Observații generale

24. Această secțiune analizează întrebările prezentate la punctul 4 de mai sus. În acest context, Comitetul va analiza, pentru întrebarea 1, compatibilitatea cu articolul 5 alineatul (1) litera (f) și cu articolele 25 și 32 din RGPD, iar pentru întrebarea 2, compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD.

25. În acest scop, Comitetul va analiza patru scenarii diferite[32], ale căror caracteristici specifice sunt descrise în secțiunea 3.2 de mai jos.

26. Ca observație preliminară, Comitetul reamintește că utilizarea datelor biometrice și, în special, a tehnologiei de recunoaștere facială implică riscuri sporite pentru drepturile și libertățile persoanelor vizate. În primul rând, prelucrarea în cauză se referă la date biometrice care beneficiază de o protecție specială în temeiul articolului 9 din RGPD. În special, datele biometrice modifică în mod ireversibil relația dintre corp și identitate, întrucât, pe baza acestor date, caracteristicile corpului uman pot fi „citite" de un dispozitiv și pot fi folosite ulterior[33]. În plus, utilizarea tehnologiei de recunoaștere facială poate genera riscuri de rezultate fals negative, prejudecăți și discriminare[34], iar potențialul de utilizare incorectă a datelor biometrice ar putea avea consecințe grave pentru persoanele implicate, cum ar fi furtul sau uzurparea identității[35]. De asemenea, ar trebui menționat faptul că, atunci când recunoașterea facială se realizează de la distanță și fără implicarea activă a persoanei vizate, aceasta din urmă ar putea fi și mai puțin conștientă de o astfel de prelucrare și de riscurile asociate. În cele din urmă, este important să se sublinieze faptul că, în general, caracteristicile pe care se bazează datele biometrice pot fi considerate permanente și ar trebui tratate ca fiind irevocabile, în special în contextul recunoașterii faciale[36].

27. Prin urmare, luând în considerare cele de mai sus, înainte de a utiliza astfel de tehnologii, chiar dacă acestea ar fi considerate deosebit de eficace, operatorii ar trebui să evalueze impactul asupra

[32] Cele patru scenarii analizate de Comitet se bazează pe cazurile de utilizare prezentate în anexa I la cerere. AS FR a clarificat faptul că aceste cazuri de utilizare prezentate în anexa I la cerere sunt exemple de punere în aplicare, aparținând unui scenariu, utilizate cu titlu ilustrativ.

[33] Avizul nr. 3/2012 al Grupului de lucru „Articolul 29" privind progresele înregistrate de tehnologiile biometrice, adoptat la 27 aprilie 2012, WP193 (denumit în continuare „**Avizul nr. 3/2012 al Grupului de lucru «Articolul 29» privind tehnologiile biometrice**"), p. 4. Trebuie menționat faptul că acest aviz face trimitere la Directiva 95/46/CE din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date („Directiva privind protecția datelor cu caracter personal"). RGPD a extins domeniul de aplicare al categoriilor speciale de date și, spre deosebire de Directiva privind protecția datelor cu caracter personal, RGPD prevede că datele biometrice sunt categorii speciale de date (articolul 9 din RGPD).

[34] Orientări privind recunoașterea facială, Comitetul consultativ privind Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, iunie 2021, p. 15; și Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctul 27.

[35] Avizul nr. 3/2012 al Grupului de lucru „Articolul 29" privind tehnologiile biometrice, p. 29.

[36] Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctul 104.

drepturilor și libertăților fundamentale ale persoanelor vizate și să analizeze dacă scopul legitim al prelucrării poate fi atins prin mijloace mai puțin intruzive[37].

28. Comitetul reamintește, de asemenea, că dreptul la protecția datelor cu caracter personal nu este un drept absolut și trebuie analizat în raport cu alte drepturi fundamentale recunoscute în Cartă, în conformitate cu principiul proporționalității[38].

29. Articolul 25 alineatul (1) din RGPD face referire la „principiile de protecție a datelor" enumerate la articolul 5 din RGPD[39] și prevede punerea în aplicare a acestora „în mod eficace" începând cu momentul conceperii[40]. Această cerință se aplică în mod expres principiului reducerii la minimum a datelor în conformitate cu articolul 5 alineatul (1) litera (c) din RGPD[41], care prevede ca datele cu caracter personal să fie „adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate, reflectând principiul proporționalității"[42]. În plus, la articolul 25 alineatul (2) din RGPD se menționează că obligația de „reducere la minimum a datelor în mod implicit" se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor[43].

---

[37] Considerentul 39 din RGPD. A se vedea, de asemenea, Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 73.

[38] Considerentul 4 din RGPD. A se vedea în acest sens și Hotărârea Curții de Justiție din 22 iunie 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (denumită în continuare „C-439/19 Latvijas Republikas Saeima"), punctele 98, 110 și 113. În plus, principiul proporționalității, ca principiu general al dreptului Uniunii, impune ca mijloacele puse în aplicare printr-un act al Uniunii să fie apte să realizeze obiectivul urmărit și să nu depășească ceea ce este necesar pentru atingerea acestuia [a se vedea Hotărârea Curții de Justiție din 9 noiembrie 2010, Volker und Markus Schecke și Eifert, C-92/09 și C-93/09, ECLI:EU:C:2010:662 (denumită în continuare „C-92/09 și C-93/09 Volker und Schecke"), punctul 74 și jurisprudența citată].

[39] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, versiunea 2.0, adoptate la 20 octombrie 2020 (denumite în continuare „**Orientările nr. 4/2019 ale CEPD privind asigurarea protecției datelor începând cu momentul conceperii și în mod implicit**"), punctul 11.

[40] Articolul 25 alineatul (1) din RGPD prevede următoarele: „Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate". A se vedea, de asemenea, Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 13.

[41] În același timp, considerentul 39 din RGPD prevede că datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace.

[42] C-439/19 Latvijas Republikas Saeima, punctul 98; Hotărârea Curții de Justiție din 11 decembrie 2019, Asociația de Proprietari bloc M5A-Scara A, C-708/18, ECLI:EU:C:2019:1064 (denumită în continuare „C-708/18 M5A-Scara A"), punctul 48.

[43] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 48.

30. Cu toate acestea, articolul 25 din RGPD nu impune operatorilor să pună în aplicare măsuri tehnice și organizatorice specifice, ci ca măsurile și garanțiile alese să fie potrivite pentru contextul și riscurile la adresa drepturilor și libertăților persoanei vizate pe care le prezintă prelucrarea în cauză[44]. În mod similar, articolul 32 din RGPD privind securitatea prelucrării impune operatorilor și persoanelor împuternicite de aceștia să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului la adresa drepturilor și libertăților persoanelor fizice.

31. Este important de reținut faptul că principiile de prelucrare consacrate în RGPD în ceea ce privește necesitatea și proporționalitatea se aplică în continuare și trebuie respectate chiar dacă pasagerii și-ar da consimțământul explicit pentru utilizarea datelor lor biometrice în scopul eficientizării fluxului de pasageri în aeroporturi[45].

32. În ceea ce privește **principiul necesității**, Comitetul va analiza dacă prelucrarea propusă este necesară pentru îndeplinirea obiectivului urmărit și dacă același obiectiv poate fi atins la fel de eficace prin alte mijloace mai puțin intruzive pentru drepturile și libertățile fundamentale ale persoanei vizate[46]. În ceea ce privește **principiul proporționalității**, Comitetul va evalua dacă impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate este proporțional cu orice beneficiu anticipat. În cazul în care beneficiul este relativ minor, este posibil ca acest impact să nu fie proporțional[47].

33. În orice caz, chiar și în situația în care Comitetul consideră că unul dintre scenariile analizate mai jos ar putea îndeplini cerințele prevăzute la articolul 5 alineatul (1) literele (e) și (f) și la articolele 25 și 32 din RGPD, este de competența operatorului în fiecare caz să demonstreze acest lucru cu elemente factuale. Această demonstrație ar trebui să includă examinarea unor scenarii alternative.

3.2 Cu privire la compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD

3.2.1 Scenariul 1: stocarea modelului biometric înregistrat exclusiv în posesia persoanei, pentru autentificare

34. În această secțiune este examinată compatibilitatea cu articolul 5 alineatul (1) litera (f) și cu articolele 25 și 32 din RGPD a stocării modelului biometric al pasagerului exclusiv în posesia acestuia, de

[44] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 14.
[45] Orientările nr. 5/2020 ale CEPD privind consimțământul în temeiul Regulamentului 2016/679, punctul 5.
[46] C-439/19 Latvijas Republikas Saeima, punctele 110 și 113; Hotărârea Curții de Justiție (Marea Cameră) din 4 iulie 2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, punctul 108.
[47] C-708/18 M5A-Scara A, punctele 52-56, C-92/09 și C-93/09 Volker und Schecke, punctul 87, C-439/19 Latvijas Republikas Saeima, punctele 98, 110 și 113. A se vedea, de asemenea, Avizul nr. 3/2012 al Grupului de lucru „Articolul 29” privind tehnologiile biometrice, p. 8.

exemplu, pe dispozitivul personal[48], sub controlul exclusiv al acestuia[49], pentru autentificare[50] (denumit în continuare „**scenariul 1**"). Această secțiune examinează, de asemenea, garanțiile adecvate pentru scenariul 1, în lumina articolelor 25 și 32 din RGPD.

Descrierea scenariului

35. În scenariul 1, modelul biometric înregistrat al fiecărui pasager care și-a dat consimțământul pentru o astfel de prelucrare este stocat exclusiv în posesia persoanei respective, de exemplu, pe un dispozitiv personal, sub controlul exclusiv al acesteia. Pasagerii sunt autentificați (comparație 1:1) atunci când trec prin anumite puncte de control din aeroport.

36. Înregistrarea este efectuată de către operatorul aeroportuar, fie de la distanță, prin intermediul aplicației acestuia[51], fie la terminalele din aeroport, cu un nivel adecvat de asigurare a încrederii (de exemplu, un nivel adecvat de asigurare conform eIDAS[52]). Aceasta constă în înregistrarea, pe dispozitivul pasagerului, a unui model biometric și a datelor de identificare[53] necesare pentru prelucrare. Înregistrarea se realizează o singură dată și pentru o anumită perioadă de valabilitate (de exemplu, aliniată la perioada de valabilitate a pașaportului pasagerilor). Nici datele de identificare, nici datele biometrice ale pasagerilor nu sunt păstrate de operatorul aeroportuar după procesul de înregistrare.

37. În special în ceea ce privește stocarea, datele de identificare și modelul biometric sunt stocate local pe dispozitivul fiecărui pasager (de exemplu, aplicația pentru dispozitive mobile a operatorului aeroportuar sau într-o aplicație de tip portofel digital). Dispozitivul poate fi apoi utilizat pentru a transmite sau a interoga datele de identificare și modelul biometric al pasagerilor, incluzând, eventual, informații privind zborul și/sau cartea de îmbarcare. De exemplu, aceste informații sunt criptate cu o cheie deținută doar de operatorul aeroportuar, posibil sub forma unui cod QR, care poate fi tipărit pe hârtie sau afișat pe ecranul dispozitivului pasagerului. În acest caz, pasagerul ar prezenta acest cod QR la echipamentele de control dedicate din aeroport, dotate cu cititor de coduri QR și cameră video.

38. Din punctul de vedere al securității, în timpul procesului de punere în corespondență, codurile QR sunt decriptate cu o cheie deținută de operatorul aeroportuar, care este singurul capabil să decripteze astfel de coduri. Datele biometrice ale pasagerilor sunt păstrate doar pentru o perioadă foarte scurtă

[48] Ca alternativă, persoana ar putea să tipărească și să își stocheze modelul biometric pe suport de hârtie.
[49] Acest lucru nu aduce atingere responsabilității generale a operatorului în ceea ce privește prelucrarea.
[50] Astfel cum este ilustrat de cazul de utilizare 1 din anexa I la cerere.
[51] CEPD precizează că, în viitor, ar putea fi avute în vedere modalități alternative de înregistrare, aceasta putând fi efectuată fără o aplicație specifică a operatorului aeroportuar, de exemplu, prin interacțiunea cu portofelul digital al utilizatorului.
[52] Un cadru pentru identificarea electronică și serviciile de încredere (denumit în continuare „**eIDAS**") bazat pe Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală.
[53] În sensul prezentului aviz, datele de identificare se referă la date precum nume, prenume, data nașterii etc., care au fost verificate ca fiind exacte pe baza unui document de identitate sau a unui pașaport.

și sunt șterse după finalizarea punerii în corespondență. Trebuie menționat faptul că măsurile de securitate în ceea ce privește stocarea depind parțial de securitatea dispozitivului pasagerului.

Evaluarea CEPD

39. Scenariul 1 descrie măsurile tehnice și organizatorice concepute pentru a asigura un nivel de securitate corespunzător riscurilor pentru persoanele vizate, astfel cum se prevede la articolul 5 alineatul (1) litera (f) și la articolul 32 din RGPD. Pasagerii sunt autentificați (comparație 1:1) atunci când trec prin anumite puncte de control din aeroport. În acest scenariu, principala operațiune de punere în corespondență se efectuează în contextul unui mediu controlat[54], în care pasagerii sunt implicați activ și au un control mai mare asupra datelor lor. În special, numai pasagerii care și-au dat consimțământul pentru o astfel de prelucrare ar fi verificați și, întrucât ar fi verificați la echipamentele de control dedicate, datele biometrice ale altor pasageri care nu și-au dat consimțământul pentru o astfel de prelucrare nu ar fi colectate. În plus, pasagerii care își dau consimțământul au posibilitatea de a opri prelucrarea în orice moment prin ștergerea datelor de pe dispozitivul lor.

40. Utilizarea recunoașterii faciale bazate pe un model biometric stocat exclusiv în posesia persoanei, de exemplu, pe un dispozitiv personal deținut de pasager, sub controlul exclusiv al acestuia, utilizat pentru autentificare la anumite puncte de control printr-o interfață dedicată, prezintă, în anumite condiții, mai puține riscuri în comparație cu o utilizare a datelor biometrice în care datele sunt stocate într-o bază de date centralizată[55]. O astfel de stocare locală, atunci când este însoțită de garanții adecvate[56], reduce gravitatea încălcărilor securității datelor cu caracter personal comparativ cu stocarea centralizată în ceea ce privește numărul de persoane afectate și asigură implicarea activă a persoanei vizate în ceea ce privește accesul la modelul biometric.

41. În plus, punerea în corespondență ar putea fi realizată local la aeroport, prin compararea modelului biometric, integrat de exemplu în codul QR, cu rezultatul modelului calculat pe baza eșantionului biometric surprins de camera video a echipamentului de control. Numai rezultatul pozitiv ar fi adus la cunoștința operatorului ce efectuează o verificare specifică (care ar putea fi un operator aeroportuar sau o companie aeriană, în funcție de locul în care are loc verificarea: punctele de control de securitate din aeroport, de predare a bagajelor, de îmbarcare și/sau de acces la salonul pentru pasageri) și ar putea fi utilizat de acesta. În plus, faptul că informațiile necesare pentru punerea în corespondență (de exemplu, codul QR) trebuie să fie furnizate de către persoana respectivă acționează ca un al doilea factor[57], sporind, astfel, securitatea autentificării.

[54] „Mediu necontrolat” se referă la utilizarea recunoașterii faciale în scopuri de identificare fără implicarea activă a persoanelor vizate, în care modelul fiecărei fețe care intră în zona de monitorizare este comparat cu modelele aparținând unui segment amplu al populației stocate într-o bază de date - a se vedea Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctul 17.

[55] Orientările nr. 5/2022 ale CEPD privind recunoașterea facială în domeniul aplicării legii, punctul 17.

[56] Astfel cum sunt descrise începând cu punctul 46 de mai jos.

[57] De exemplu, atenuează riscul de fraudare a identității. A se vedea, de asemenea, garanția C.1.2 de mai jos.

42. În ceea ce privește compatibilitatea cu articolul 25 din RGPD și, în special, pentru a respecta cerința de reducere la minimum a datelor, ar trebui să se asigure faptul că prelucrarea respectă principiul necesității. În scenariul 1, s-ar putea considera că măsurile alese respectă principiul necesității în raport cu scopul urmărit (eficientizarea fluxului de pasageri) dacă, în funcție de circumstanțele prelucrării, operatorul poate demonstra că nu există soluții alternative mai puțin intruzive care ar permite atingerea aceluiași obiectiv într-un mod la fel de eficace. De exemplu, operatorul poate demonstra că, deși pasagerii ar fi nevoiți să își prezinte dispozitivul, scenariul 1 accelerează procesul de verificare în comparație cu situația actuală, care include o verificare umană a corespondenței dintre numele de pe cartea de îmbarcare și cel din documentul de identitate al pasagerului[58]. În special, acest lucru nu ar putea fi demonstrat în situația în care, în prezent, nu se efectuează niciun control pentru a verifica identitatea pasagerilor pe baza documentului lor oficial de identitate (a se vedea, în această privință, punctul 18 de mai sus).

43. În plus, modelele biometrice nu sunt păstrate de operatorul aeroportuar după înregistrare, iar perioada de păstrare a datelor biometrice de către operatorul care efectuează verificarea este foarte scurtă, aceste date fiind șterse imediat după finalizarea punerii în corespondență. Astfel, măsurile alese în scenariul 1 par să limiteze amploarea prelucrării și perioada de stocare a datelor cu caracter personal.

44. În ceea ce privește principiul proporționalității, caracterul intruziv al unei astfel de prelucrări poate fi contrabalansat de implicarea activă a pasagerilor, întrucât datele biometrice ale acestora ar fi stocate exclusiv în posesia acestora. În plus, ținând seama de măsurile descrise mai sus și presupunând că operatorul pune în aplicare garanții adecvate, necesare pentru prelucrarea în cauză, implementarea unor măsuri adecvate ar putea asigura un nivel de securitate corespunzător riscului. În acest caz, impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate ar putea fi considerat proporțional cu beneficiul anticipat.

45. Prin urmare, având în vedere cele de mai sus, ca răspuns la întrebarea 1.1, Comitetul concluzionează că o astfel de prelucrare **ar putea fi considerată, în principiu, compatibilă cu articolul 5 alineatul (1) litera (f) și cu articolele 25 și 32 din RGPD, sub rezerva punerii în aplicare a unor garanții adecvate**.

Garanții adecvate

46. În acest tip de scenariu, ca răspuns la întrebarea 1.2, CEPD consideră că ar trebui puse în aplicare cel puțin următoarele garanții. Ar putea fi instituite și alte garanții decât cele descrise în prezentul aviz pentru a atinge aceleași obiective de securitate și de protecție a datelor și acestea ar putea fi legale atât timp cât respectă cadrul juridic aplicabil.

47. Notă: aceasta este o imagine de ansamblu la nivel înalt și neexhaustivă a posibilelor garanții adecvate care ar trebui puse în aplicare de un operator într-o soluție similară scenariului 1. Caracterul adecvat al acestora în temeiul articolelor 25 și 32 din RGPD va fi analizat de la caz la caz. Toți operatorii vor

[58] De asemenea, s-ar putea susține că verificarea biometrică poate fi mai puțin predispusă la erori decât o verificare umană.

trebui să efectueze propria evaluare a impactului asupra protecției datelor (denumită în continuare „EIPD”)[59], iar soluțiile lor specifice pot necesita măsuri suplimentare care nu sunt incluse în prezentul aviz.

A. Generalități

A.1 Evaluarea impactului prelucrării datelor

A.1.1 Efectuarea unei EIPD, în conformitate cu articolul 35 din RGPD, ori de câte ori operatorul planifică o nouă operațiune de prelucrare care este susceptibilă să genereze un risc ridicat. Acest lucru poate fi valabil în cazul scenariului 1, deoarece implică prelucrarea pe scară largă a datelor biometrice[60]. Evaluarea oportunității implementării unui sistem de recunoaștere facială, inclusiv a necesității și a proporționalității acestuia în legătură cu scopurile urmărite[61], în faza timpurie a conceperii și revizuirea acestuia pe parcursul întregului ciclu de dezvoltare a produsului;

A.1.2 Consultarea autorității de supraveghere relevante în cazul în care prelucrarea generează un risc ridicat în pofida măsurilor luate de operator pentru atenuarea riscului[62].

A.2 Drepturile persoanelor vizate și garanțiile care pot fi puse în aplicare de către operatori

A.2.1 Garanții pentru abordarea rezultatelor fals negative. Atenuarea riscului de părtinire pe criterii de vârstă, gen și rasă prin „evaluarea cu regularitate dacă algoritmii funcționează în conformitate cu scopurile, ajustarea algoritmilor pentru reducerea erorilor sistematice descoperite și asigurarea echității prelucrării”[63]. De exemplu, prin implementarea supravegherii și a intervenției umane, în vederea atenuării oricăror prejudecăți și a prevenirii stigmatizării sau creării de profiluri ale pasagerilor;

A.2.2 Asigurarea transparenței tuturor operațiunilor de prelucrare de date cu caracter personal și a faptului că persoanele vizate cunosc și controlează modalitățile în care le sunt prelucrate datele în cadrul fiecărei operațiuni de prelucrare[64];

A.2.3 Adoptarea unor măsuri de asigurare a respectării principiului limitării scopului, astfel încât datele să nu fie utilizate în alte scopuri, cum ar fi în scopuri de securitate sau de formare;

[59] Articolul 35 din RGPD.
[60] Articolul 35 alineatul (3) din RGPD și Orientările Grupului de lucru „Articolul 29” privind evaluarea impactului asupra protecției datelor (EIPD) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679, adoptate la 13 octombrie 2017, WP 248 rev. 01, aprobate de CEPD.
[61] Articolul 35 alineatul (7) litera (b) din RGPD.
[62] Articolul 36 alineatul (1) din RGPD.
[63] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, nota de subsol 60, punctul 70.
[64] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 68 și considerentul 7 din RGPD.

A.2.4 Adoptarea unor măsuri adecvate de prevenire a realizării de fotografii sau capturi video, chiar dacă acestea nu sunt înregistrate sau prelucrate, cu persoanele care nu și-au dat consimțământul pentru utilizarea recunoașterii faciale (măsurile pot include utilizarea unei adâncimi a câmpului și a unei zonei de captare adecvate pentru a evita captarea de imagini cu alți pasageri aflați în fundal sau în zona din jur, implementarea unor culoare specifice pentru recunoașterea facială, semnalizate clar);

A.2.5 În cazul în care este posibil ca aceleași echipamente de control să fie folosite atât de pasagerii care și-a dat consimțământul, cât și de cei care nu și-au dat consimțământul pentru utilizarea recunoașterii faciale sau atunci când este posibil ca pasagerii care nu și-au dat consimțământul pentru utilizarea recunoașterii faciale să apară în câmpul vizual în timp ce sistemul nu este utilizat, realizarea fotografiei sau captarea video să aibă loc numai după o acțiune pozitivă din partea unui pasager care și-a dat consimțământul;

A.2.6 Posibilitatea unei persoane vizate de a șterge în orice moment datele care se află exclusiv în posesia sa (model biometric[65]), și anume într-o aplicație pentru dispozitive mobile sau într-un portofel digital[66];

A.2.7 Existența unor alternative viabile sau a unor soluții de rezervă (de exemplu, pentru pasagerii care nu își dau consimțământul pentru utilizarea datelor lor biometrice, care nu pot utiliza astfel de soluții sau care fac obiectul unor respingeri eronate), astfel încât pasagerii care nu își dau consimțământul să nu sufere niciun prejudiciu[67];

A.2.8 Dacă se utilizează o aplicație, aceasta ar trebui să fie concepută și configurată cu atenție pentru a nu colecta date inutile și pentru a evita utilizarea oricăror kituri de dezvoltare de software („SDK") ale unor terți, care colectează date în alte scopuri.

A.3 Responsabilitate

A.3.1 Evaluarea existenței unor coduri de conduită sau a unor mecanisme de certificare relevante care pot fi utilizate ca elemente prin care să se demonstreze îndeplinirea cerințelor legate de securitatea prelucrării prevăzute la articolul 32 din RGPD[68]. Verificarea caracterului adecvat al măsurilor pentru prelucrarea specifică în cauză. Standardele[69], bunele practici și

[65] Trimiterile la modelul biometric din garanțiile pentru scenariul 1 corespund trimiterilor la cheia/metoda secretă din scenariul 2.
[66] Rețineți că această garanție este valabilă numai în scenariul 1.
[67] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 86.
[68] Articolul 32 alineatul (3) din RGPD și Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 10.
[69] A se vedea, de exemplu, ISO/IEC 2382-37.

codurile de conduită recunoscute de asociații și de alte organisme care reprezintă categoriile de operatori de date pot ajuta la stabilirea măsurilor adecvate;

A.3.2 Efectuarea unor controale de securitate de bază pe dispozitivul utilizatorilor pentru a permite înregistrarea, chiar dacă și pasagerul are un rol în protecția datelor sale, acestea fiind stocate pe dispozitivul său. Exemple de astfel de verificări și controale tehnice sunt prezentate mai jos în secțiunea C.2 „Infrastructură și rețea".

B. Măsuri organizatorice:

B.1 Politică și conformitate

B.1.1. Instituirea de controale interne ale accesului[70] cu reguli pentru administratori;

B.1.2 Atunci când serviciul de recunoaștere facială poate fi prestat de una din părțile implicate în prelucrare fără a fi necesară gestionarea datelor de identificare, a datelor biometrice sau a ambelor tipuri de date de către celelalte părți implicate, interzicerea transmiterii datelor respective către aceste părți. De exemplu, nu este necesar din punct de vedere tehnic ca o companie aeriană să acceseze datele biometrice atunci când se bazează pe infrastructura aeroportuară comună, chiar dacă respectiva companie aeriană acționează în calitate de operator al prelucrării în temeiul RGPD;

B.1.3 Definirea unei politici de criptare și gestionare a cheilor[71], de exemplu, pentru prelucrarea datelor de identificare și a datelor biometrice;

B.1.4 Asigurarea conformității cu dispozițiile capitolului V din RGPD. De exemplu, pentru a asigura transferuri conforme atunci când operatorul utilizează un serviciu la distanță cu sediul într-o țară terță în timpul procesului de înregistrare;

B.1.5 Atunci când prelucrarea este realizată de o persoană împuternicită de operator, existența unui contract care reglementează relația acesteia cu operatorul[72] în conformitate cu articolul 28 alineatul (3) din RGPD;

[70] Orientările nr. 4/2020 ale CEPD privind utilizarea datelor de localizare și a instrumentelor de urmărire a contactelor în contextul pandemiei de COVID-19, adoptate la 21 aprilie 2020 (denumite în continuare „**Orientările nr. 4/2020 ale CEPD privind datele de localizare și instrumentele de urmărire a contactelor**"), SEC-10, p. 16.
[71] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 89.
[72] Articolul 28 alineatul (3) din RGPD.

B.1.6 Instituirea unor proceduri de asigurare a supravegherii și intervenției umane, în special pentru soluționarea problemelor legate de respingerile eronate și a problemelor tehnice sau de utilizare.

B.2 Formare și testare

B.2.1. Asigurarea formării corespunzătoare a personalului;

B.2.2 Implementarea unui „proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării”[73];

B.2.3. Implementarea unui proces pentru a se asigura că prelucrarea modelului biometric al pasagerului[74] în scopul autentificării este eficace din punct de vedere tehnic și suficient de precisă;

B.2.4. Asigurarea faptului că eșantioanele biometrice colectate atât în momentul înregistrării, cât și la punctul de control au o calitate suficientă pentru o prelucrare fiabilă a datelor biometrice.

C. Măsuri tehnice:

C.1 Acces

C.1.1 Punerea în aplicare a unor garanții în faza de înregistrare pentru a asigura un proces de înregistrare bazat pe metoda *bootstrap* cu o identitate verificată. De exemplu, pot fi puse în aplicare diverse măsuri pentru a consolida evaluarea autentificării multifactoriale a identității utilizatorilor, de la linkuri unice protejate prin parolă pentru activarea aplicației până la mecanisme locale de deblocare a dispozitivelor;

C.1.2 Punerea în aplicare a unor garanții pentru abordarea rezultatelor fals pozitive, pentru combaterea perturbării sistemului biometric prin manipularea imaginilor faciale și pentru prevenirea fraudei[75];

C.1.3 Interzicerea accesului extern la datele de identificare și la datele biometrice[76];

C.1.4 Asigurarea prelucrării locale în fazele de înregistrare, transmitere și punere în corespondență. Punctul de punere în corespondență ar trebui să fie cât mai aproape de dispozitivul persoanei în cauză. Punerea în corespondență a modelului biometric pe

[73] Articolul 32 alineatul (1) litera (d) din RGPD.
[74] Trimiterile la modelul biometric din garanțiile pentru scenariul 1 corespund trimiterilor la cheia/metoda secretă din scenariul 2.
[75] Raportul ENISA „Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust” (Identitatea digitală: utilizarea conceptului de identitate autonomă pentru consolidarea încrederii), ianuarie 2022.
[76] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 89.

dispozitivul pasagerului ar putea necesita interacțiunea cu furnizori de servicii din afara aeroportului și utilizarea resurselor rețelei publice, dezavantajul în acest caz fiind afectarea disponibilității și transmiterea modelului către entități externe;

C.1.5 Autentificarea unui utilizator pentru adăugarea unui nou zbor și generarea unui nou cod QR criptat;

C.1.6 Adoptarea unor măsuri pentru abordarea situației în care un pasager nu mai are acces la codul său QR.

C.2 Infrastructură și rețea

C.2.1 Actualizarea permanentă a condițiilor privind sistemul de operare („SO") și activarea autentificării pentru a permite accesul la dispozitiv și funcționarea aplicației/portofelului digital, inclusiv ștergerea automată a datelor de identificare și a datelor biometrice în cazul în care sistemul de operare este învechit și prezintă riscuri de securitate;

C.2.2 Izolarea de rețea a unităților de punere în corespondență (adică, echipamentele de control) în timpul utilizării și luarea oricăror altor măsuri necesare pentru asigurarea securității;

C.2.3 Compararea datelor biometrice pe dispozitivul pasagerului sau la echipamentul de control (edge computing);

C.2.4 Soluții pentru abordarea vulnerabilităților în materie de securitate ale dispozitivelor personale ale pasagerilor, inclusiv criptarea (cel puțin) a datelor biometrice și de identificare în repaus;

C.2.5 Stocarea securizată (cel puțin) a datelor biometrice exclusiv la dispoziția utilizatorului[77], de exemplu prin utilizarea unei enclave securizate pe un telefon inteligent;

C.2.6 Garanții de securitate pentru a asigura securitatea fizică în incinta aeroportului, inclusiv la terminalul de comparare a datelor biometrice din aeroport. Asigurarea unui nivel ridicat de securitate a acelor elemente ale arhitecturii care prelucrează datele de identificare și datele biometrice (de exemplu, calcul, flux de date, stocarea tranzitorie sau pe termen lung).

C.3 Securitatea și gestionarea datelor privind controlul identității utilizatorilor

[77] Trimiterile la modelul biometric din garanțiile pentru scenariul 1 corespund trimiterilor la cheia/metoda secretă din scenariul 2.

C.3.1 Compartimentarea datelor în timpul transmiterii și stocării în cel puțin trei grupuri diferite, cum ar fi: date de identificare, date biometrice și date legate de zbor[78]. Asigurarea criptării corespunzătoare a datelor între transmitere și stocare;

C.3.2 Implementarea unor măsuri tehnice pentru a se asigura că numai datele care pot fi prelucrate legal la puncte de control specifice sunt prelucrate și verificate la punctele de control respective;

C.3.3 Asigurarea eficacității ștergerii datelor[79] printr-o procedură de ștergere securizată (de exemplu, memorie principală, memorie cache, posibile copii de rezervă) și evaluarea situațiilor în care datele trebuie să fie șterse automat. Perioadele de stocare a datelor ar trebui să fie aplicate strict prin proceduri automate, fără a fi necesară o acțiune suplimentară din partea persoanei[80];

C.3.4 Asigurarea autenticității și integrității datelor (de exemplu, semnătura)[81];

C.3.5 Păstrarea datelor biometrice ale pasagerilor la punctul de înregistrare și la punctul de control numai pentru o perioadă foarte scurtă de timp și ștergerea acestora imediat ce pasagerul trece prin punctul de control;

C.3.6 În cazul în care pentru înregistrare este utilizată o aplicație, aplicarea unor standarde pentru securitatea aplicațiilor mobile în timpul dezvoltării acesteia, precum și teste de securitate efectuate de un terț;

C.3.7 Instituirea unor măsuri de securitate în timpul fazei de înregistrare la aeroport pentru asigurarea confidențialității și a integrității datelor biometrice ale pasagerului. De exemplu, în cazul în care codul QR este tipărit de ghișeu, acesta nu ar trebui să fie afișat la ghișeu pentru a evita fotografierea acestuia de către un actor rău intenționat. În cazul unei transmisii cu rază scurtă de acțiune, aceasta ar trebui efectuată cu implicarea activă a utilizatorului și printr-un canal care să asigure proximitatea;

C.3.8 Datele aflate exclusiv în posesia persoanei respective[82] ar trebui stocate în mod securizat pe dispozitivul acesteia, iar eventualele vulnerabilități legate de sistemele de operare ale dispozitivului trebuie să fie remediate prin corecții de securitate adecvate. În cazul unui cod

[78] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 89.
[79] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 89.
[80] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 82.
[81] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 89.
[82] Trimiterile la modelul biometric din garanțiile pentru scenariul 1 corespund trimiterilor la cheia/metoda secretă din scenariul 2.

QR tipărit, persoana ar trebui să fie informată cu privire la natura sensibilă a datelor pe care le conține și la ce oferă acces acesta;

C.3.9 Asigurarea faptului că înregistrarea este efectuată pe baza unor tehnici adecvate de dovedire a identității de la distanță[83].

3.2.2 Scenariul 2: stocarea centralizată, în cadrul aeroportului, a unui model biometric înregistrat într-o formă criptată, cu o cheie/metodă secretă aflată exclusiv în posesia pasagerului respectiv, pentru autentificare

48. În această secțiune este examinată compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD a stocării centralizate, în vederea autentificării, a modelelor biometrice înregistrate ale pasagerilor într-o bază de date centralizată, într-o formă criptată și cu o cheie/metodă secretă aflată exclusiv în posesia pasagerului respectiv[84] (denumit în continuare „**scenariul 2**"). Această secțiune examinează, de asemenea, garanțiile adecvate pentru scenariul 2, în lumina articolelor 25 și 32 din RGPD.

Descrierea scenariului

49. În scenariul 2, înregistrarea se efectuează o singură dată, pentru o anumită perioadă (de exemplu, un an de la data ultimului zbor și până la data expirării pașaportului), fie de la distanță, cu un nivel adecvat de asigurare a încrederii (de exemplu, un nivel adecvat de asigurare conform eIDAS), fie la terminalele din aeroport. Înregistrarea este controlată de operatorul aeroportuar și constă în generarea de date de identificare și de date biometrice criptate cu o cheie/metodă secretă.

50. Baza de date este stocată în incinta aeroportului, sub controlul operatorului aeroportuar. Cheile/metodele secrete de criptare individuale sunt stocate exclusiv pe dispozitivul persoanei respective (de exemplu, în aplicația pentru dispozitive mobile a operatorului aeroportuar). Aplicația poate genera un cod QR ce conține cheia/metoda secretă, care poate fi tipărit pe hârtie sau afișat pe ecranul dispozitivului[85]. În plus, un al doilea nivel de criptare[86] este asigurat de operatorul aeroportuar prin chei controlate de acesta.

51. Pasagerii sunt autentificați (comparație 1:1) atunci când trec prin anumite puncte de control din aeroport. Pasagerii care aleg să treacă prin punctele de control biometric prezintă codul QR la un echipament de control special prevăzut cu un cititor de coduri QR și o cameră video. Indexul pasagerului este trimis în baza de date pentru a obține modelul criptat, care este descărcat și verificat

[83] A se vedea Raportul ENISA „Remote ID Proofing: Analysis of methods to carry out identity proofing remotely" (Dovedirea identității la distanță: analiza metodelor de dovedire a identității de la distanță), martie 2021.
[84] Astfel cum este ilustrat de cazul de utilizare 2 din anexa I la cerere.
[85] AS FR a clarificat, de asemenea, că ar putea exista și alte soluții tehnice pentru transmiterea informațiilor necesare, cum ar fi utilizarea unui protocol de comunicații cu rază scurtă de acțiune.
[86] Cheia/metoda secretă (aflată exclusiv în posesia persoanei respective) este la rândul său criptată cu o altă cheie deținută de operatorul aeroportuar.

local la echipamentul de control și/sau pe dispozitivul utilizatorului. Numai rezultatul pozitiv este adus la cunoștința operatorului punctului de control și este utilizat de acesta[87].

52. În acest scenariu, nu există fluxuri de date de identificare și de date biometrice între aeroporturi și nici interconectare sau interoperabilitate între bazele de date centralizate.

Evaluarea CEPD

53. În scenariul 2, modelele biometrice înregistrate ale pasagerilor sunt stocate centralizat, dar într-o formă criptată și cu o cheie/metodă secretă aflată exclusiv în posesia acestora. În scenariul 2, pasagerii sunt autentificați (comparație 1:1).

54. În acest scenariu, se propune ca obiectivul de eficientizare a fluxului de pasageri (prin asigurarea unor controale mai rapide) să fie atins prin utilizarea unui sistem centralizat. CEPD a precizat anterior că o astfel de soluție ar putea fi considerată o alternativă viabilă la stocarea descentralizată a modelelor biometrice înregistrate[88] (astfel cum se descrie în scenariul 1), cu condiția să existe nevoi obiective și să fie puse în aplicare garanții adecvate (a se vedea garanțiile descrise începând cu punctul 60 de mai jos).

55. În ceea ce privește aspectele de securitate, datele fiecărei persoane sunt criptate cu cheia specifică deținută numai de persoana respectivă și aflată sub controlul exclusiv al acesteia. În plus, faptul că informațiile necesare pentru punerea în corespondență (și anume metoda secretă/cheia) trebuie să fie furnizate de către persoana respectivă acționează ca un al doilea factor[89], sporind, astfel, securitatea autentificării. În plus, un al doilea nivel de criptare este asigurat de operatorul aeroportuar prin chei controlate de acesta. În scenariul 2, indexul persoanei este trimis în baza de date centrală în vederea extragerii datelor biometrice asociate persoanei respective. Aceste date sunt apoi trimise (criptate) către un computer de la punctul de control, unde sunt decriptate pentru a realiza punerea în corespondență și numai rezultatul pozitiv este adus la cunoștința operatorului și utilizat de acesta. Prin urmare, aceste măsuri de securitate ar putea fi considerate compatibile cu articolul 5 alineatul (1) litera (f) și cu articolul 32 din RGPD, cu condiția ca cheia/metoda secretă asociată persoanei respective să fie păstrată în computerul de la punctul de control și ca numai indexul pasagerului să fie trimis în baza de date centrală pentru obținerea modelului biometric criptat.

56. În ceea ce privește compatibilitatea cu articolul 25 din RGPD și, în special, pentru a respecta cerința de reducere la minimum a datelor, ar trebui să se asigure faptul că prelucrarea respectă principiul necesității. În scenariul 2, s-ar putea considera că măsurile alese respectă principiul necesității în raport cu scopul urmărit (eficientizarea fluxului de pasageri în aeroporturi) dacă, în funcție de circumstanțele prelucrării, operatorul poate demonstra că nu există soluții alternative mai puțin intruzive care ar permite atingerea aceluiași obiectiv într-un mod la fel de eficace. Și în scenariul 2

[87] AS FR a clarificat faptul că această perioadă de stocare este furnizată în scop ilustrativ și poate fi considerată acceptabilă de vreme ce cheia se află în posesia persoanelor respective și ar putea fi aleasă în faza de înregistrare. Cu toate acestea, trebuie menționat faptul că această perioadă de stocare poate fi modificată.
[88] Ghidul nr. 3/2019 al CEPD privind mijloacele video, punctul 88.
[89] De exemplu, atenuează riscul de fraudare a identității. A se vedea, de asemenea, garanția C.1.2.

pasagerii ar fi nevoiți să își prezinte dispozitivul[90]. Cu toate acestea, operatorul poate demonstra că scenariul 2 accelerează procesul de verificare în comparație cu situația actuală, care include o verificare umană a corespondenței dintre numele de pe cartea de îmbarcare și cel din documentul de identitate al pasagerului[91] sau în comparație cu scenariul 1. În special, acest lucru nu ar putea fi demonstrat în situația în care, în prezent, nu se efectuează niciun control pentru a verifica identitatea pasagerilor pe baza documentului lor oficial de identitate (a se vedea, în această privință, punctul 18 de mai sus).

57. În ceea ce privește principiul proporționalității, caracterul intruziv al unei astfel de prelucrări poate fi contrabalansat de implicarea activă a pasagerilor, cheia asociată datelor lor criptate fiind sub controlul exclusiv al acestora. În plus, se pare că riscurile de securitate pe care le implică stocarea datelor biometrice ale pasagerilor într-o bază de date centralizată, cheia aflându-se sub controlul exclusiv al acestora, pot fi atenuate prin utilizarea unor garanții adecvate (a se vedea garanțiile descrise începând cu punctul 60 de mai jos). Prin urmare, presupunând că operatorul pune în aplicare garanții adecvate, necesare pentru prelucrarea în cauză, riscurile pentru pasageri ar putea fi atenuate, iar impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate ar putea fi considerat proporțional cu beneficiul anticipat. Bineînțeles că trebuie să se asigure în fiecare caz că sunt prelucrate numai datele necesare pentru îndeplinirea scopului urmărit și că numai pasagerii care și-au dat consimțământul vor fi verificați, astfel încât să nu existe niciun risc ca datele biometrice ale altor pasageri, care nu și-au dat consimțământul, să fie colectate.

58. În cerere se menționează ca exemplu faptul că, în scenariul 2, perioada de stocare a datelor criptate în baza de date ar putea fi, de regulă, un an de la ultimul zbor efectuat de persoana respectivă și până la data expirării pașaportului. Nu sunt furnizate însă informații pentru a justifica o perioadă atât de lungă pe baza unor motive obiective, deși se poate presupune că o astfel de perioadă de stocare este avută în vedere din motive practice pentru zborurile viitoare. În ceea ce privește perioada de stocare, pentru a asigura compatibilitatea cu articolul 5 alineatul (1) litera (e) din RGPD în acest scenariu, operatorii ar trebui să poată justifica de ce această perioadă de păstrare este necesară pentru îndeplinirea scopului prelucrării în cazuri specifice. Comitetul recomandă operatorilor să aibă în vedere cea mai scurtă perioadă de stocare posibilă, luând în considerare și pasagerii care zboară foarte rar și să le ofere persoanelor vizate opțiunea de a-și alege perioada de stocare preferată.

59. Având în vedere aceste aspecte, ca răspuns la întrebarea 2.1.1, Comitetul concluzionează că o astfel de prelucrare **ar putea fi considerată, în principiu, compatibilă cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD, sub rezerva punerii în aplicare a unor garanții adecvate**.

Garanții adecvate

60. În acest tip de scenariu, ca răspuns la întrebarea 2.1.2, Comitetul consideră că, **pe lângă garanțiile menționate în scenariul 1**, ar trebui puse în aplicare cel puțin următoarele garanții. Ar putea fi instituite și alte garanții decât cele descrise în prezentul aviz pentru a atinge aceleași obiective de

[90] AS FR a clarificat, de asemenea, că ar putea exista și alte opțiuni de prezentare a unui model, de exemplu, tipărit pe hârtie. În plus, CEPD recunoaște că, în viitor, ar putea fi avută în vedere utilizarea unei tehnologii alternative, de exemplu, bazate pe un sistem de comunicare în câmp apropiat.

[91] De asemenea, s-ar putea susține că verificarea biometrică poate fi mai puțin predispusă la erori decât o verificare umană.

securitate și de protecție a datelor, iar acestea ar putea fi legale atât timp cât respectă cadrele juridice aplicabile.

61. Notă: *aceasta este o imagine de ansamblu la nivel înalt și neexhaustivă a posibilelor garanții adecvate care ar putea fi puse în aplicare de un operator într-o soluție similară scenariului 2. Caracterul adecvat al acestora în temeiul articolelor 25 și 32 din RGPD va fi analizat de la caz la caz. Toți operatorii vor trebui să efectueze propria evaluare a impactului asupra protecției datelor, iar soluțiile lor specifice pot necesita măsuri suplimentare care nu sunt incluse în prezentul aviz.*

D. Generalități

D.1 Drepturile persoanelor vizate și garanțiile care pot fi puse în aplicare de către operatori

D.1.1 Asigurarea faptului că pasagerul deține controlul asupra perioadelor de stocare a tuturor datelor sale. Perioadele de stocare ar trebui limitate la ceea ce este necesar pentru scopul respectiv. Ar trebui stabilită o perioadă maximă în urma unei analize aprofundate a mai multor factori, precum perioada de valabilitate a documentului de identificare. Persoanelor vizate ar trebui să li se ofere posibilitatea de a-și stabili perioada de stocare preferată, care poate fi mai scurtă decât perioada de stocare implicită;

D.1.2 Posibilitatea unei persoane vizate de a solicita în orice moment ștergerea datelor care se află exclusiv în posesia sa (cheie/metodă secretă), și anume într-o aplicație pentru dispozitive mobile sau într-un portofel digital[92];

D.1.3 Asigurarea faptului că localizarea bazei de date centrale permite autorității de supraveghere competente să efectueze o supraveghere eficace a acesteia.

E. Măsuri organizatorice:

E.1 Politică și conformitate

E.1.1 Încrederea în serverul central trebuie să fie limitată. Asigurarea faptului că gestionarea serverului central respectă norme de guvernanță clar definite și include toate măsurile necesare pentru asigurarea securității acestuia[93].

F. Măsuri tehnice:

F.1 Acces

[92] Rețineți că această garanție este valabilă numai în scenariul 2.
[93] Orientările nr. 4/2020 ale CEPD privind datele de localizare și instrumentele de urmărire a contactelor, PRIV-5, p. 17.

F.1.1 Păstrarea de înregistrări cu persoanele care au acces la datele cu caracter personal, în special la datele de identificare și datele biometrice, precum și cu momentul accesării acestora;

F.2 Infrastructură și rețea

F.2.1 Asigurarea securității corespunzătoare a bazei de date centrale, inclusiv împotriva atacurilor la disponibilitate;

F.2.2 Asigurarea faptului că nu există nicio conexiune de internet la baza de date centrală, la echipamentele de înregistrare și la unitățile de punere în corespondență. Operarea și întreținerea acestui sistem (de exemplu, copii de rezervă, corecții, monitorizare etc.) trebuie să se realizeze la nivel local, în incinta aeroportului.

F.3 Securitatea și gestionarea datelor

F.3.1 Folosirea unor tehnici criptografice de ultimă generație pentru securizarea schimburilor dintre aplicație și serverul centralizat[94];

F.3.2 Păstrarea cheii/metodei secrete individuale în locul în care va fi utilizată pentru decriptare (și anume la echipamentul de control) și utilizarea indexului numai pentru extragerea modelului biometric înregistrat corespunzător din baza de date centrală;

F.3.3 Asigurarea schimbului de cheie/metodă secretă între dispozitivul utilizatorului și echipamentul de control protejează comunicarea împotriva eventualelor interceptări sau transmiteri către terți;

F.3.4 Indexarea modelului biometric atunci când este stocat în baza de date centrală pentru a permite autentificarea 1:1 și pentru a se asigura că acesta este unic și asociat persoanei respective. Asigurarea faptului că indexul nu dezvăluie niciuna dintre informațiile de identificare ale pasagerului și nu este corelat cu cheia de criptare;

F.3.5 Autentificarea și criptarea corespunzătoare a oricărei transmisii între baza de date centrală și punctele de control și folosirea de rețele izolate în acest scop;

F.3.6 Evitarea legăturilor bidirecționale dintre seturile de date (date de identificare și date biometrice, precum și detalii despre zbor) și păstrarea în baza de date doar a legăturilor unidirecționale relevante. De exemplu, doar a legăturilor unidirecționale de

[94] Orientările nr. 4/2020 ale CEPD privind datele de localizare și instrumentele de urmărire a contactelor, SEC-4, p. 16: „Printre tehnicile care pot fi utilizate se numără: criptarea simetrică și asimetrică, funcțiile *hash*, testul de apartenență la un domeniu privat, intersectarea seturilor private, filtrele Bloom, extragerea de informații cu caracter privat, criptarea homomorfică”.

la index la datele de identificare, de la index la datele biometrice criptate și de la index la detaliile despre zbor;

F.3.7 Instituirea unor mecanisme de asigurare a continuității activității, de exemplu prin implementarea unor sisteme de stocare de rezervă adecvate;

F.3.8 Asigurarea faptului că echipamentul de control nu păstrează înregistrări ale modelelor criptate sau necriptate.

3.2.3 Stocarea centralizată a modelelor biometrice înregistrate pentru identificare

62. În această secțiune este examinată compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din RGPD a stocării centralizate, în vederea identificării, a modelelor biometrice înregistrate ale pasagerilor, atunci când aceste modele nu sunt criptate cu o cheie/metodă secretă aflată exclusiv în posesia pasagerilor respectivi, în două cazuri de utilizare: (1) atunci când aceste modele sunt stocate într-o bază de date din cadrul aeroportului, sub controlul operatorului aeroportuar[95] (situație denumită în continuare „**scenariul 3.1**”) și (2) atunci când aceste modele sunt stocate în cloud, sub controlul companiei aeriene[96] (situație denumită în continuare „**scenariul 3.2**”).

63. Comitetul consideră că utilizarea datelor biometrice în scopuri de **identificare** în baze de date centrale de mari dimensiuni interferează cu drepturile fundamentale ale persoanelor vizate și ar putea avea consecințe grave pentru acestea[97]. În plus, utilizarea datelor biometrice ar trebui examinată, de asemenea, în raport cu scopul în care acestea sunt prelucrate, având în vedere principiile necesității și proporționalității[98].

3.2.3.1 Scenariul 3.1: stocarea centralizată într-o bază de date în cadrul aeroportului, sub controlul operatorului aeroportuar

Descrierea scenariului

64. În scenariul 3.1, modelul biometric înregistrat al pasagerilor este stocat într-o formă criptată într-o bază de date centrală în incinta aeroportului și sub controlul operatorului aeroportuar. În plus, datele pasagerilor sunt compartimentate, ceea ce înseamnă că datele lor de identificare, modelul lor biometric înregistrat și informațiile despre zbor sunt stocate în trei baze de date diferite. Aceste date sunt criptate cu chei diferite, atât în timpul stocării, cât și în timpul transmiterii către serverele care realizează punerea în corespondență, unde sunt apoi decriptate de operatorul aeroportuar.

65. Pasagerii trebuie să se înregistreze pentru fiecare zbor, cu puțin timp înainte de plecare (de exemplu, 48 de ore). Înregistrarea poate fi efectuată fie de la distanță, fie la terminalele din aeroport, cu un

[95] Astfel cum este ilustrat de cazul de utilizare 3A din anexa I la cerere.
[96] Astfel cum este ilustrat de cazul de utilizare 3B din anexa I la cerere.
[97] A se vedea, de exemplu, Avizul nr. 3/2012 al Grupului de lucru „Articolul 29” privind tehnologiile biometrice, p. 8. A se vedea, de asemenea, punctul 26 de mai sus.
[98] Considerentul 4 din RGPD. A se vedea, de asemenea, Avizul nr. 3/2012 al Grupului de lucru „Articolul 29” privind tehnologiile biometrice, p. 8.

nivel adecvat de asigurare a încrederii (de exemplu, un nivel adecvat de asigurare conform eIDAS). Ca alternativă, înregistrarea poate fi efectuată la fel ca în scenariul 1, caz în care pasagerii trebuie să își transfere datele din portofelele lor digitale către sistemul aeroportuar cu maximum 48 de ore înainte de plecare.

66. Și în acest scenariu pasagerii se prezintă la un echipament de control dedicat, prevăzut cu o cameră video. Eșantionul lor biometric este trimis apoi către un server central al aeroportului, care va încerca să compare datele cu cele din baza centrală de date biometrice. Astfel, pasagerul poate fi identificat și se poate verifica dacă acesta este sau nu înregistrat pentru un zbor de plecare (sau pentru zborul respectiv, în cazul controlului la îmbarcare). În funcție de punctul de control, datele trimise înapoi operatorului solicitant pot fi reduse la minimum, putând lua, de exemplu, forma unui răspuns „da/nu" sau a rezultatului pozitiv efectiv, dacă este necesar. În acest caz, numai rezultatul cererii este transmis operatorului punctului de control și utilizat de acesta.

67. Mai concret, acest scenariu se referă la identificarea pasagerilor (comparație 1:N), unde N este numărul preconizat de pasageri din aeroport într-un interval de mai multe zile. În plus, compararea datelor biometrice se efectuează numai atunci când un pasager se prezintă la punctele de control predefinite din aeroportul de plecare, însă prelucrarea efectivă a datelor are loc într-un server central conectat la baza de date centrală. Perioada de stocare în acest scenariu este, de regulă, de 48 de ore, iar datele sunt șterse după decolarea avionului.

Evaluarea CEPD

68. Astfel cum s-a reamintit mai sus, prelucrarea datelor biometrice implică riscuri sporite pentru drepturile și libertățile persoanelor vizate[99]. Astfel, orice deficiență în materie de securitate a datelor poate avea consecințe deosebit de grave pentru persoanele vizate[100]. Operatorii sunt obligați să atenueze eficient aceste riscuri. Întrucât, în acest scenariu, întreaga arhitectură este complet centralizată, pasagerii pierd într-o mai mare măsură controlul asupra datelor lor. În plus, poate crește și riscul ca datele să fie prelucrate în alte scopuri decât controlul fluxului de pasageri.

69. Având în vedere principiul securității și cerințele în materie de securitate [articolul 5 alineatul (1) litera (f) și articolul 32 din RGPD], ar trebui luat în considerare faptul că stocarea datelor de identificare și a datelor biometrice în baze de date centrale, fie ele și separate, poate trezi interesul actorilor rău intenționați, iar compromiterea confidențialității bazei de date poate genera ulterior riscul accesării întregului set de date. În consecință, o posibilă încălcare a securității în ceea ce privește modelele de recunoaștere facială și datele de identificare asociate poate permite identificarea neautorizată sau ilegală a persoanelor vizate în alte medii. De asemenea, în funcție de metodele utilizate pentru identificarea biometrică, aceasta poate reprezenta o amenințare la adresa utilizării în continuare, în condiții de siguranță, a modelelor de recunoaștere facială ca identificator. În acest caz, efectele încălcării nu pot fi atenuate, spre deosebire de alte tipuri de date de autentificare (de exemplu, nume de utilizator, parolă) care pot fi modificate[101].

[99] A se vedea punctul 26 de mai sus.
[100] Orientări privind recunoașterea facială, Comitetul consultativ privind Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, iunie 2021, p. 22.
[101] A se vedea, în acest sens, Avizul nr. 3/2012 al Grupului de lucru „Articolul 29" privind tehnologiile biometrice, p. 34.

70. În plus, volumul mare și nivelul ridicat de calitate a datelor de identificare și a datelor biometrice deținute de operator fac din acestea o țintă foarte valoroasă pentru un atacator, fapt care crește riscul în materie de securitate. În plus, încălcările securității datelor ar putea avea un impact mai mare, întrucât stocarea centralizată a datelor ar putea facilita accesul atacatorilor la datele cu caracter personal referitoare la mai mulți pasageri. Prin urmare, o posibilă încălcare ar putea expune un număr mare de persoane vizate la riscuri ridicate din punct de vedere al gravității, de exemplu, furtul de identitate pe scară largă, care sunt extrem de dificil de atenuat.

71. Prin urmare, în ceea ce privește compatibilitatea cu articolul 5 alineatul (1) litera (f) și cu articolul 32 din RGPD, ținând seama de stadiul actual al tehnologiei, măsurile avute în vedere în scenariul 3.1[102] sunt insuficiente pentru a asigura un nivel de securitate corespunzător riscului. Pe această bază, prelucrarea efectuată în cadrul scenariului 3.1 nu ar respecta nici articolul 5 alineatul (1) litera (f), nici articolul 32 din RGPD dacă un operator s-ar limita la aceste măsuri.

72. Având în vedere principiul prevăzut la articolul 5 alineatul (1) litera (e) din RGPD, în acest scenariu, perioada de stocare a datelor biometrice în baza de date centrală este, de regulă, de 48 de ore. Această limitare a stocării pare să reducă în mod semnificativ riscurile asociate încălcării securității datelor cu caracter personal. Cu toate acestea, perioada de stocare a datelor nu este în sine un factor decisiv pentru compatibilitatea globală a arhitecturii menționate, întrucât perioadele de păstrare pot fi modificate de operatori. În orice caz, măsurile propuse trebuie să respecte cerințele privind protecția datelor începând cu momentul conceperii și în mod implicit în temeiul articolului 25 din RGPD.

73. Spre deosebire de scenariile 1 și 2, în care pasagerii sunt autentificați, în scenariul 3.1 pasagerii sunt identificați (comparație 1:N), unde N este numărul preconizat de pasageri în aeroport într-un interval de mai multe zile, pasageri care și-au dat consimțământul pentru o astfel de prelucrare atunci când trec prin anumite puncte de control din aeroport. Acest lucru implică căutarea pasagerilor într-o bază de date centrală, prin prelucrarea fiecărui eșantion biometric colectat pentru a verifica dacă acesta corespunde unei persoane cunoscute de sistem. Spre deosebire de scenariul 2, în scenariul 3.1, cheile nu se află exclusiv în posesia pasagerilor. În consecință, în acest scenariu, pasagerii au un control mult mai redus asupra datelor lor biometrice. Prin urmare, prelucrarea propusă în scenariul 3.1 nu poate fi compatibilă cu cerințele privind protecția datelor începând cu momentul conceperii și în mod implicit în temeiul articolului 25 din RGPD.

74. În lumina articolului 25 din RGPD, operatorii trebuie să ia în considerare tipurile, categoriile și nivelul de detaliu al datelor cu caracter personal necesare în scopul prelucrării[103]. Alegerile în materie de proiectare trebuie să țină cont de riscurile sporite pentru principiul reducerii la minimum a datelor, al integrității și al confidențialității și de limitările legate de stocare atunci când se colectează volume mari de date cu caracter personal detaliate, iar toate acestea trebuie comparate cu reducerea riscurilor prin colectarea unor volume mai mici de informații și/sau a unor informații mai puțin detaliate despre persoanele vizate. Indiferent de situație, configurația implicită nu trebuie să includă colectarea de date cu caracter personal care nu sunt necesare pentru scopul specific al prelucrării. Cu alte cuvinte, dacă anumite categorii de date cu caracter personal nu sunt necesare sau dacă nu sunt necesare date detaliate pentru că este suficientă existența unor date mai puțin rafinate, atunci restul

[102] Astfel cum sunt descrise la punctele 64-67 de mai sus.

[103] Orientările nr. 4/2019 ale CEPD privind asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 49.

de date cu caracter personal nu se mai colectează. În acest caz, dacă o altă modalitate de prelucrare ar putea atinge același obiectiv și este disponibilă în conformitate cu termenii descriși în scenariul 3.1, utilizarea tehnologiei de recunoaștere facială nu este necesară.

75. În ceea ce privește articolul 25 din RGPD, un element principal legat de protecția datelor începând cu momentul conceperii și în mod implicit este autonomia persoanei vizate. În special, persoanei vizate trebuie să i se acorde cel mai înalt nivel posibil de autonomie pentru a stabili modul în care îi sunt utilizate datele cu caracter personal, precum și domeniul de aplicare și condițiile utilizării sau prelucrării respective[104]. În scenariul 1, persoana vizată ar avea autonomie și control în ceea ce privește utilizarea, divulgarea și ștergerea modelelor sale biometrice, iar în scenariul 2, persoana vizată ar menține un anumit control în ceea ce privește divulgarea modelului său biometric, întrucât cheia/metoda secretă de criptare s-ar afla în posesia acesteia. Cu toate acestea, în scenariul 3.1, persoana vizată depinde pe deplin de alegerile operatorului în ceea ce privește prelucrarea datelor sale biometrice și, prin urmare, nu are niciun control direct asupra utilizării modelului său biometric.

76. În ceea ce privește compatibilitatea cu articolul 25 din RGPD și, în special, pentru a respecta cerința de reducere la minimum a datelor, prelucrarea avută în vedere în scenariul 3.1 nu poate respecta principiul necesității. Comitetul consideră că un efect similar în ceea ce privește eficientizarea fluxului de pasageri în aeroporturi poate fi obținut într-un mod mai puțin intruziv asupra vieții private. De exemplu, acest efect poate fi obținut fără utilizarea datelor biometrice (deși experiența utilizatorului ar fi diferită în acest caz, deoarece prezentarea cărții de îmbarcare și, dacă este necesar, a documentelor oficiale de identificare ar putea necesita un timp mai lung). În plus, alte soluții, în special cele bazate pe stocarea datelor biometrice într-un portofel local pe dispozitivul persoanei respective sau cele care implică criptarea datelor cu o cheie specifică stocată pe dispozitivul persoanei respective, permit atingerea obiectivelor într-un mod mai puțin intruziv asupra vieții private.

77. În ceea ce privește principiul proporționalității, prelucrarea avută în vedere în scenariul 3.1 ar genera riscuri pentru drepturile persoanelor vizate care nu ar fi atenuate prin măsurile prezentate, ținând seama de stadiul actual al tehnologiei. Impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate care ar putea rezulta din încălcarea securității datelor biometrice ale unui număr mare de persoane stocate într-o bază de date centralizată pare să depășească beneficiul anticipat al prelucrării, care este unul relativ minor, și anume o ușoară creștere a confortului și a vitezei controalelor. Prin urmare, nivelul ridicat de intruziune al acestor măsuri în ceea ce privește drepturile și libertățile fundamentale ale persoanelor nu poate fi justificat, iar prelucrarea avută în vedere în scenariul 3.1 nu respectă principiul proporționalității.

78. Având în vedere aceste aspecte, ca răspuns la întrebarea 2.2.1, Comitetul concluzionează că, atunci când este efectuată în scopul specific al eficientizării fluxului de pasageri în aeroporturi, prelucrarea prevăzută în scenariul 3.1:

- **nu poate fi compatibilă cu articolul 25 din RGPD**;
- **nu ar respecta nici articolul 5 alineatul (1) litera (f), nici articolul 32 din RGPD** dacă un operator s-ar limita la măsurile descrise în scenariul 3.1.

[104] Orientările nr. 4/2019 ale CEPD privind asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 70. Considerentul 7 din RGPD clarifică, de asemenea, faptul că „persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal”.

3.2.3.2 Scenariul 3.2: stocarea centralizată în cloud, sub controlul companiei aeriene

Descrierea scenariului

79. În scenariul 3.2, modelul biometric înregistrat al pasagerilor este stocat în cloud, sub controlul companiei aeriene sau al furnizorului de servicii de cloud al acesteia (persoana împuternicită de operator). În cerere se precizează că furnizorul de servicii de cloud ar fi situat în SEE[105]. În acest caz, datele pasagerilor sunt criptate, dar vor fi decriptate atunci când sunt utilizate (de exemplu, atunci când se efectuează punerea în corespondență), iar cheile se află sub controlul companiei aeriene sau al furnizorului de servicii de cloud al acesteia. Datele biometrice ale pasagerilor sunt utilizate pentru identificarea acestora (comparație 1:N), unde N reprezintă un număr mai mic decât sau potențial egal cu numărul total al clienților companiei aeriene[106].

80. La fel ca în scenariile 1, 2 și 3.1, și în acest caz pasagerii trebuie să se înregistreze în prealabil. Cu toate acestea, în scenariul 3.2, înregistrarea pasagerilor se realizează o singură dată și pentru o perioadă echivalentă cu perioada în care clientul deține un cont la compania aeriană. Înscrierea se efectuează fie de la distanță, cu un nivel adecvat de asigurare a încrederii (de exemplu, un nivel adecvat de asigurare conform eIDAS), fie la terminalele din aeroport. Compararea datelor biometrice se efectuează numai atunci când pasagerii se prezintă la punctele de control predefinite din aeroport, însă prelucrarea efectivă a datelor are loc în cloud.

81. La aeroport, pasagerii trec prin puncte de control dedicate, echipate cu o cameră video. Datele biometrice ale pasagerilor sunt transmise printr-o cerere către un server cloud al companiei aeriene, unde sunt comparate cu cele din baza de date centrală. Astfel, pasagerul poate fi identificat și se poate verifica dacă acesta este sau nu înregistrat pentru un zbor de plecare (sau pentru zborul respectiv în cazul controlului la îmbarcare).

82. Este posibil ca rezultatele pozitive să fie puse la dispoziția mai multor operatori aeroportuari în cazul în care o companie aeriană are un terminal dedicat sau are acces la infrastructura sistemului informatic comun al unui aeroport. În funcție de punctul de control, datele trimise înapoi operatorului solicitant pot fi reduse la minimum, putând lua, de exemplu, forma unui răspuns „da/nu” sau chiar a rezultatului pozitiv, dacă este necesar. În acest caz, numai rezultatul cererii este adus la cunoștința operatorului și utilizat de acesta.

83. Perioada de stocare a modelului este definită de compania aeriană și poate fi echivalentă cu perioada în care clientul deține un cont la compania aeriană.

Evaluarea CEPD

[105] AS FR a clarificat faptul că este vorba de un exemplu ilustrativ și că ar putea fi luați în considerare și furnizorii de servicii de cloud care nu sunt situați în SEE. În plus, ar putea fi avute în vedere și alte soluții de stocare (de exemplu, fără utilizarea serviciilor de cloud).
[106] AS FR a clarificat faptul că este vorba de un exemplu ilustrativ și că există o soluție prin care datele biometrice sunt transmise de fiecare dată înainte de zbor.

84. Considerațiile deja exprimate de Comitet în legătură cu scenariul 3.1[107] se aplică și în acest scenariu.

85. În ceea ce privește principiul securității și cerințele în materie de securitate [articolul 5 alineatul (1) litera (f) și articolul 32 din RGPD], în scenariul 3.2 prelucrarea are loc în cloud, mai multe entități putând avea acces la date, inclusiv, eventual, furnizori din afara SEE, chiar și atunci când datele sunt deținute în SEE[108]. O astfel de arhitectură implică riscuri potențiale în ceea ce privește transferurile de date cu caracter personal către țări terțe. În plus, deși datele pasagerilor sunt criptate, acestea sunt decriptate atunci când sunt utilizate (și anume atunci când se efectuează punerea în corespondență), iar cheile se află sub controlul companiei aeriene sau al furnizorului de servicii de cloud al acesteia. O astfel de stocare poate crește riscurile de încălcare a securității datelor.

86. Prin urmare, în ceea ce privește compatibilitatea cu articolul 5 alineatul (1) litera (f) și cu articolul 32 din RGPD, ținând seama de stadiul actual al tehnologiei, măsurile avute în vedere în scenariul 3.2[109] sunt insuficiente pentru a asigura un nivel de securitate corespunzător riscului. Pe această bază, prelucrarea efectuată în cadrul scenariului 3.2 nu ar respecta nici articolul 5 alineatul (1) litera (f), nici articolul 32 din RGPD dacă un operator s-ar limita la aceste măsuri.

87. În plus, conform scenariului 3.2[110], datele ar putea fi stocate pentru o perioadă mare de timp (și anume o perioadă care poate fi echivalentă cu perioada în care persoana vizată deține un cont la compania aeriană). O asemenea durată de stocare crește riscurile de încălcare a confidențialității și a integrității datelor și pare să depășească ceea ce este strict necesar și proporțional în scopul prelucrării. Comitetul precizează că perioada de stocare a datelor nu este în sine un factor decisiv pentru compatibilitatea globală a arhitecturii menționate cu dispozițiile RGPD, întrucât poate fi modificată de operatorii de date. Cu toate acestea, pe baza informațiilor de care dispune Comitetul și cuprinse în descrierea scenariului 3.2, nu există o justificare suficientă pentru această perioadă lungă de păstrare și nicio măsură aparentă de atenuare a riscurilor pentru pasageri. Pe această bază, perioada de stocare propusă nu ar fi limitată la ceea ce este necesar, în conformitate cu principiul limitării legate de stocare prevăzut la articolul 5 alineatul (1) litera (e) din RGPD.

88. În orice caz, măsurile propuse în scenariul 3.2 nu pot îndeplini cerințele privind protecția datelor începând cu momentul conceperii și în mod implicit în temeiul articolului 25 din RGPD. În scenariul 3.2, modelele biometrice înregistrate ale pasagerilor sunt stocate în cloud, sub controlul companiei aeriene sau al furnizorului de servicii de cloud al acesteia (persoana împuternicită de operator). Astfel cum s-a descris mai sus, mai multe entități ar putea avea acces la aceste date. În plus, datele biometrice ale pasagerilor sunt utilizate pentru identificarea acestora (comparație 1:N), unde N reprezintă până la numărul total al utilizatorilor/clienților companiei aeriene. Această metodă implică găsirea unei persoane dintr-un grup de persoane în baza de date centrală, prin prelucrarea fiecărei fețe surprinse pentru a verifica dacă aceasta corespunde unei persoane cunoscute de sistem. Spre deosebire de scenariul 3.1, în scenariul 3.2 comparația ar putea fi efectuată la o scară mult mai mare, deoarece criteriul în acest caz este numărul total de clienți ai companiei aeriene, în timp ce

[107] Punctele 68-77 de mai sus.
[108] Acțiunea coordonată privind asigurarea respectării legii 2022 a CEPD – Utilizarea serviciilor bazate pe cloud de către sectorul public, 17 ianuarie 2023, p. 19.
[109] A se vedea punctele 79-83 de mai sus.
[110] A se vedea punctul 83 de mai sus.

scenariul 3.1 a inclus doar numărul preconizat de pasageri în aeroport într-un interval de mai multe zile.

89. În plus, în ceea ce privește compatibilitatea cu articolul 25 din RGPD și, în special, pentru a respecta cerința de reducere la minimum a datelor, prelucrarea avută în vedere în scenariul 3.2 nu poate respecta principiul necesității. Comitetul consideră că un efect similar în ceea ce privește eficientizarea fluxului de pasageri în aeroporturi ar putea fi obținut prin alte măsuri mai puțin intruzive, de exemplu fără utilizarea datelor biometrice, deși experiența utilizatorului ar fi diferită în acest caz, deoarece prezentarea documentului de identitate și a cărții de îmbarcare ar putea necesita un timp mai lung. În plus, alte soluții, în special cele bazate pe stocarea datelor biometrice într-un portofel local pe dispozitivul persoanei respective sau cele care implică criptarea datelor cu o cheie specifică stocată pe dispozitivul persoanei respective, îi permit operatorului să îndeplinească obiectivele într-un mod mai puțin intruziv asupra vieții private.

90. În ceea ce privește principiul proporționalității, prelucrarea avută în vedere în scenariul 3.2 ar genera riscuri pentru drepturile persoanelor vizate care nu ar fi atenuate prin garanțiile prezentate. Impactul negativ asupra drepturilor și libertăților fundamentale ale persoanelor vizate care ar rezulta din încălcarea securității datelor biometrice ale unui număr mare de persoane stocate într-o bază de date centralizată în cloud pare să depășească beneficiul anticipat al prelucrării, care este unul relativ minor, și anume o ușoară creștere a confortului și a vitezei controalelor. Prin urmare, nivelul ridicat de intruziune al acestor măsuri în ceea ce privește drepturile și libertățile fundamentale ale persoanelor nu poate fi justificat, iar prelucrarea avută în vedere în scenariul 3.2 nu poate fi considerată proporțională.

91. Având în vedere aceste aspecte, ca răspuns la întrebarea 2.3.1, Comitetul concluzionează că, atunci când este efectuată în scopul specific al eficientizării fluxului de pasageri în aeroporturi, prelucrarea prevăzută în scenariul 3.2:

- **nu poate fi compatibilă cu articolul 25 din RGPD**;
- **nu ar respecta nici articolul 5 alineatul (1) litera (f), nici articolul 32 din RGPD** dacă un operator s-ar limita la măsurile descrise în scenariul 3.2;
- **nu ar respecta articolul 5 alineatul (1) litera (e) din RGPD**, întrucât, pe baza informațiilor de care dispune Comitetul, nu există o justificare suficientă pentru perioada de păstrare prevăzută în scenariul 3.2. Pentru a respecta principiul limitării legate de stocare prevăzut la articolul 5 alineatul (1) litera (e) din RGPD, operatorul ar trebui să demonstreze că datele cu caracter personal nu sunt stocate pe o perioadă care depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate.

4 CONCLUZII

92. În ceea ce privește întrebarea 1.1, pe baza cererii de aviz formulate de AS FR, în legătură cu cerințele de la articolul 5 alineatul (1) litera (f) și de la articolele 25 și 32 din RGPD și pe baza analizei de mai sus, Comitetul concluzionează că:

93. utilizarea tehnologiei de recunoaștere facială pentru autentificarea bazată pe date biometrice, cu scopul specific de a eficientiza fluxul de pasageri în aeroporturi (punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri) ar putea, în principiu, să fie considerată compatibilă cu principiul integrității și al confidențialității în temeiul articolului 5 alineatul (1) litera (f) și al articolelor 25 și 32 din RGPD în cazul unei arhitecturi de stocare în care modelul biometric

înregistrat al fiecărui pasager este stocat local, pe dispozitivul personal și sub controlul exclusiv al acestuia, sub rezerva punerii în aplicare a unor garanții adecvate descrise începând cu punctul 46 de mai sus.

94. În ceea ce privește întrebarea 2.1.1, pe baza cererii de aviz formulate de AS FR, în legătură cu cerințele prevăzute la articolul 5 alineatul (1) literele (e) și (f) și la articolele 25 și 32 din RGPD și pe baza analizei de mai sus, Comitetul concluzionează că:

95. utilizarea tehnologiei de recunoaștere facială pentru autentificarea bazată pe date biometrice, cu scopul specific de a eficientiza fluxul de pasageri în aeroporturi (punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri) ar putea, în principiu, să fie considerată compatibilă cu principiul limitării legate de stocare în temeiul articolului 5 alineatul (1) litera (e) și cu principiul integrității și al confidențialității în temeiul articolului 5 alineatul (1) litera (f) și al articolelor 25 și 32 din RGPD în cazul unei arhitecturi de stocare centralizată în care modelul biometric înregistrat al fiecărui pasager este stocat într-o bază de date centrală din cadrul aeroportului, sub controlul operatorului aeroportuar, într-o formă criptată, cu o cheie/metodă secretă aflată exclusiv în posesia persoanei respective, sub rezerva punerii în aplicare a unor garanții adecvate descrise începând cu punctul 60 de mai sus.

96. În ceea ce privește întrebarea 2.2.1, pe baza cererii de aviz formulate de AS FR, în legătură cu cerințele prevăzute la articolul 5 alineatul (1) literele (e) și (f) și la articolele 25 și 32 din RGPD și pe baza analizei de mai sus, Comitetul concluzionează că:

97. utilizarea tehnologiei de recunoaștere facială pentru identificarea bazată pe date biometrice, cu scopul specific de a eficientiza fluxul de pasageri în aeroporturi (punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri) în cazul unei arhitecturi de stocare centralizată în care modelele biometrice înregistrate ale pasagerilor nu sunt criptate cu o cheie/metodă secretă aflată exclusiv în posesia fiecărui pasager și sunt stocate într-o bază de date în cadrul aeroportului (sub controlul operatorului aeroportuar) nu poate fi compatibilă cu articolul 25 din RGPD. De asemenea, o astfel de prelucrare nu ar respecta principiul integrității și al confidențialității în temeiul articolului 5 alineatul (1) litera (f) și al articolului 32 din RGPD dacă un operator s-ar limita la măsurile descrise în scenariul 3.1.

98. În ceea ce privește întrebarea 2.3.1, pe baza cererii de aviz formulate de AS FR, în legătură cu cerințele prevăzute la articolul 5 alineatul (1) literele (e) și (f) și la articolele 25 și 32 din RGPD și pe baza analizei de mai sus, Comitetul concluzionează că:

99. utilizarea tehnologiei de recunoaștere facială pentru identificarea bazată pe date biometrice, cu scopul specific de a eficientiza fluxul de pasageri în aeroporturi (punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri) în cazul unei arhitecturi de stocare centralizată în care modelele biometrice înregistrate ale pasagerilor nu sunt criptate cu o cheie/metodă secretă aflată exclusiv în posesia fiecărui pasager și sunt stocate în cloud (sub controlul companiei aeriene) nu poate fi compatibilă cu articolul 25 din RGPD. De asemenea, o astfel de prelucrare nu ar respecta principiul integrității și al confidențialității în temeiul articolului 5 alineatul (1) litera (f) și al articolului 32 din RGPD dacă un operator s-ar limita la măsurile descrise în scenariul 3.2. În cele din urmă, pe baza descrierii scenariului 3.2 și a informațiilor de care dispune Comitetul, prelucrarea nu ar respecta principiul limitării legate de stocare prevăzut la articolul 5 alineatul (1) litera (e) din RGPD.

Pentru Comitetul european pentru protecția datelor,

Președinte

(Anu Talus)