

Kolēģijas atzinums (64. pants)



**Atzinums 11/2024 par sejas atpazīšanas tehnoloģiju
izmantošanu, lai racionalizētu pasažieru plūsmu lidostās
(saderība ar VDAR 5. panta 1. punkta e) un f) apakšpunktu,
25. un 32. pantu)**

Versija 1.1

Pieņemts 2024. gada 23. maijā

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

Versija 1.1	2024. gada 28. maijs	Gramatisks labojums kopsavilkumā (3. un 4. lpp.) un atzinuma 77. un 90. punktā
Versija 1.0	2024. gada 23. maijs	Atzinuma pieņemšana

Kopsavilkums

Francijas uzraudzības iestāde lūdza Eiropas Datu aizsardzības kolēģiju sniegt atzinumu par to, kā lidostu ekspluatanti un aviosabiedrības izmanto sejas atpazīšanas tehnoloģijas pasažieru autentificēšanai vai identifikācijai, izmantojot biometriskos datus, lai racionalizētu pasažieru plūsmu lidostās.

Vispirms kolēģija atgādina, ka biometrisko datu un jo īpaši sejas atpazīšanas tehnoloģijas izmantošana nozīmē paaugstinātu risku datu subjektu tiesībām un brīvībām. Tas attiecas uz tādu biometrisko datu apstrādi, kam saskaņā ar VDAR 9. pantu ir piešķirta īpaša aizsardzība. Pat ja šādas tehnoloģijas tiktu uzskatītas par īpaši efektīvām, pirms to izmantošanas pārziņiem būtu jānovērtē ietekme uz datu subjektu pamattiesībām un brīvībām un jāapsver, vai apstrādes leģitīmo nolūku var īstenot ar mazāk ierobežojošiem līdzekļiem.

Šā atzinuma darbības joma, kā norādīts lūgumā, attiecas tikai uz tādas apstrādes saderību ar **VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu**, kuras mērķis ir četros konkrētos kontrolpunktos, proti, drošības kontrolpunktos, bagāžas nodošanas punktos, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpām, **racionalizēt pasažieru plūsmu lidostās**. Šajā atzinumā nav iekļauta pilnīga analīze par to, kā katrā atsevišķā gadījumā attiecīgais(-ie) pārzinis(-ņi), kā arī attiecīgā gadījumā datu apstrādātājs(-i) ievēro VDAR. Tāpēc šis atzinums neskar individuālu gadījumu juridisku un tehnisku analīzi, kuras pamatā ir pārziņa paredzētā konkrētā apstrāde un apstākļi. Turklāt piemērojamā juridiskā pamata analīze nav to jautājumu lokā, kas kolēģijai uzdoti pieprasījumā, un līdz ar to piekrišanas šādai apstrādei spēkā esamība saskaņā ar VDAR 6., 7. un 9. pantu šajā atzinumā nav izvērtēta. Turklāt šis atzinums neskar dalībvalstu tiesību aktos paredzētos biometrisko datu izmantošanas ierobežojumus.

Šajā atzinumā kolēģija izvērtē apstrādes atbilstību iepriekš minētajiem VDAR noteikumiem saistībā ar **četriem konkrētiem scenārijiem**.

Pirmais scenārijs ietver reģistrētas biometriskās veidnes glabāšanu pie attiecīgās personas, piemēram, tās individuālajā ierīcē, kas atrodas tikai šīs personas kontrolē, lai autentificētu (tieši salīdzinātu) pasažieri, kad viņš ierodas iepriekš minētajos lidostas kontrolpunktos.

Kolēģija secina, ka izvēlētos pasākumus varētu uzskatīt par tādiem, kas atbilst nepieciešamības principam, ja pārzinis var pierādīt, ka nav mazāk ierobežojošu alternatīvu risinājumu, ar kuriem tikpat efektīvi varētu sasniegt to pašu mērķi. Turklāt datu apstrādes radītos ierobežojumus var līdzsvarot ar pasažieru aktīvu iesaisti, jo tikai viņi uzglabā savu biometrisko veidni, piemēram, savā individuālajā ierīcē, kas atrodas tikai attiecīgās personas kontrolē, un viņu dati tiek dzēsti īsi pēc atbilstības meklēšanas beigām. Uz šā pamata kolēģija secina, ka pirmajā scenārijā paredzēto apstrādi **principā varētu uzskatīt par saderīgu ar VDAR 5. panta 1. punkta f) apakšpunktu, 25. un 32. pantu**, ja tiek īstenotas atbilstošas garantijas.

Kolēģija ir noteikusi minimālās garantijas, kuras būtu jāīsteno saistībā ar risinājumu, kas līdzīgs pirmajam scenārijam.

Otrais scenārijs ietver reģistrētas un šifrētas biometriskās veidnes centralizētu glabāšanu lidostā, atslēgai / slepenajai parolei atrodoties tikai pie pasažiera. Tas ļauj veikt pasažieru autentifikāciju (tiešu

salīdzināšanu), kad viņi ierodas iepriekš minētajos lidostas kontrolpunktos. Reģistrācija ir derīga noteiktu laikposmu, kas, piemēram, varētu būt ne vairāk kā viens gads pēc pēdējā lidojuma līdz pases derīguma termiņa beigām.

Kolēģija secina, ka apstrādi varētu uzskatīt par tādu, kas atbilst nepieciešamības principam, ja pārzinis var pierādīt, ka nav mazāk ierobežojošu alternatīvu risinājumu, ar kuriem tikpat efektīvi varētu sasniegt to pašu mērķi. Turklāt apstrādes radītos ierobežojumus var kompensēt ar pasažiera aktīvu iesaisti, jo viņa šifrēto biometrisko datu atslēga / slepenā parole atrodas tikai pie pasažiera. Pieņemot, ka pārzinis īsteno atbilstošas garantijas, drošības risku, ko šī scenārija gadījumā rada centralizētas datubāzes izmantošana, varētu mazināt un negatīvo ietekmi uz datu subjektu pamattiesībām un brīvībām varētu uzskatīt par proporcionālu paredzamajam ieguvumam. Saistībā ar glabāšanas ierobežojuma principu kolēģijai nav sniegta nekāda informācija, kas pamatotu ilgo glabāšanas laiku. Lai šā scenārija gadījumā panāktu saderību ar VDAR 5. panta 1. punkta e) apakšpunktu, pārziņiem būtu jāspēj pamatot, kāpēc paredzētais glabāšanas periods konkrētos gadījumos ir nepieciešams, lai īstenotu šo nolūku. Kolēģija iesaka pārziņiem paredzēt pēc iespējas īsāku glabāšanas laiku, vienlaikus piedāvājot pasažieriem iespēju noteikt savu vēlamo glabāšanas laiku. Uz šā pamata kolēģija secina, ka otrajā scenārijā paredzēto apstrādi **principā varētu uzskatīt par saderīgu ar VDAR 5. panta 1. punkta e) un f) apakšpunktu, 25. un 32. pantu**, ja tiek īstenotas atbilstošas garantijas.

Kolēģija ir noteikusi minimālās garantijas, kuras būtu jāīsteno saistībā ar risinājumu, kas līdzīgs otrajam scenārijam.

Trešais scenārijs ietver reģistrētas un šifrētas biometriskās veidnes centralizētu glabāšanu lidostā tās ekspluatanta kontrolē. Tas ļauj veikt pasažieru identifikāciju (salīdzināšanu attiecībā 1:N), kad viņi ierodas iepriekš minētajos lidostas kontrolpunktos. Šajā scenārijā paredzētais glabāšanas laiks parasti ir 48 stundas, un dati tiek dzēsti, tiklīdz lidmašīna ir pacēlusies.

Tā kā identifikācijas un biimetriskie dati tiek glabāti centrālā datubāzē, datubāzes konfidencialitātes apdraudējuma gadījumā var tikt gūta piekļuve visam datu kopumam, kā arī var rasties iespēja neatļauti vai nelikumīgi identificēt pasažierus citās situācijās. Lidostas ekspluatanta kontrolē esošās centralizētās glabāšanas arhitektūras dēļ pasažieris arī lielākā mērā zaudē kontroli pār saviem datiem. Kolēģija uzskata, ka attiecībā uz pasažieru plūsmas racionalizēšanu lidostās līdzīgu rezultātu var sasniegt ar mazākiem ierobežojumiem, un šķiet, ka negatīvā ietekme uz datu subjektu pamattiesībām un brīvībām, ko radītu datu aizsardzības pārkāpums centralizētā biometrisko datu datubāzē, ir lielāka par paredzamo ieguvumu no apstrādes. Tāpēc apstrāde nevar atbilst nepieciešamības un proporcionalitātes principiem. Uz šā pamata kolēģija secina, ka trešajā scenārijā paredzētā apstrāde **nevar būt saderīga ar VDAR 25. pantu**. Tā arī **neatbilstu VDAR 5. panta 1. punkta f) apakšpunktam un 32. pantam**, ja pārzinis izmantotu tikai šajā scenārijā aprakstītos pasākumus.

Ceturtais scenārijs ietver reģistrētas un šifrētas biometriskās veidnes centralizētu glabāšanu mākonī, ko kontrolē aviosabiedrība vai tās mākoņpakalpojumu sniedzējs. Tas ļauj veikt pasažieru identifikāciju (salīdzināšanu attiecībā 1:N), kad viņi ierodas iepriekš minētajos lidostas kontrolpunktos. Glabāšanas periods šajā scenārijā var būt tik ilgs, cik vien ilgi klientam ir konts aviosabiedrībā.

Tā kā identifikācijas un biimetrisko datu glabāšana mākonī notiek centrālā datubāzē, šādiem datiem varētu piekļūt vairākas struktūras, tostarp, iespējams, tādi pakalpojumu sniedzēji, kas atrodas ārpus EEZ. Pasažiera datus atšifrē, kad tos izmanto, un atslēgas ir aviosabiedrības vai tās datu apstrādātāju kontrolē, un tas varētu palielināt drošības apdraudējumiem pakļauto datu daļu. Šāda centralizēta

glabāšanas arhitektūra arī nozīmē, ka pasažieris lielākā mērā zaudē kontroli pār saviem datiem. Datus arī varētu glabāt ievērojamu laika periodu, kas tiem radītu augstāku drošības pārkāpumu risku, un šķiet, ka tas pārsniedz to, kas ir absolūti nepieciešams un samērīgs apstrādes nolūkos, ja vien netiek veikti turpmāki acīmredzami pasākumi, lai mazinātu risku personām.

Kolēģija uzskata, ka attiecībā uz pasažieru plūsmas racionalizēšanu lidostās līdzīgu rezultātu var sasniegt ar mazākiem ierobežojumiem, un šķiet, ka negatīvā ietekme uz datu subjektu pamattiesībām un brīvībām, ko varētu radīt datu aizsardzības pārkāpums centralizētā biometrisko datu datubāzē, ir lielāka par paredzamo ieguvumu no apstrādes. Tāpēc apstrāde nevar atbilst nepieciešamības un proporcionalitātes principiem. Uz šā pamata kolēģija secina, ka ceturtajā scenārijā paredzētā apstrāde **nevar būt saderīga ar VDAR 25. pantu**. Tā arī **neatbilstu VDAR 5. panta 1. punkta e) apakšpunktam**, pamatojoties uz kolēģijai pieejamo informāciju, kā arī **VDAR 5. panta 1. punkta f) apakšpunktam un 32. pantam**, ja pārzinis izmantotu tikai šajā scenārijā aprakstītos pasākumus.

Satura rādītājs

1	IEVADS.....	6
1.1	Faktu kopsavilkums.....	6
1.2	Pieprasījuma sniegt atzinumu saskaņā ar VDAR 64. panta 2. punktu pieņemamība.....	8
2	ATZINUMA DARBĪBAS JOMA UN KONTEKSTS.....	9
2.1	Atzinuma darbības joma	9
2.2	Galvenie jēdzieni.....	12
3	Par pieprasījuma pamatotību	14
3.1	Vispārējas piezīmes.....	14
3.2	Par saderību ar VDAR 5. panta 1. punkta e) un f) apakšpunktu, 25. un 32. pantu	16
3.2.1	1. scenārijs – reģistrētās biometriskās veidnes glabāšana tikai pie attiecīgās personas, lai veiktu autentifikāciju.....	16
3.2.2	2. scenārijs – reģistrētās biometriskās veidnes centralizēta glabāšana šifrētā veidā lidostā, atslēgai / slepenajai parolei atrodoties tikai pie pasažiera, lai veiktu autentifikāciju	24
3.2.3	Reģistrēto biometrisko veidņu centralizēta glabāšana, lai veiktu identifikāciju	29
3.2.3.1	<i>3.1. scenārijs – centralizēta glabāšana lidostā esošā datubāzē lidostas ekspluatanta kontrolē</i> 29	
3.2.3.2	<i>3.2. scenārijs – centralizēta glabāšana mākonī aviosabiedrības kontrolē</i>	33
4	SECINĀJUMI.....	35

Eiropas Datu aizsardzības kolēģija

Ņemot vērā 63. pantu un 64. panta 2. punktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk – **VDAR**),

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018¹,

ņemot vērā Eiropas Datu aizsardzības kolēģijas (turpmāk – **kolēģija** jeb **EDAK**) reglamenta (turpmāk – **EDAK reglaments**) 10. un 22. pantu,

tā kā:

(1) Kolēģijas galvenais uzdevums ir nodrošināt konsekventu VDAR piemērošanu visā Eiropas Ekonomikas zonā (turpmāk – **EEZ**). VDAR 64. panta 2. punktā ir noteikts, ka jebkura uzraudzības iestāde (turpmāk – **UI**), kolēģijas priekšsēdētājs vai Komisija var pieprasīt, lai kolēģija izskata jebkuru jautājumu par vispārējo piemērošanu vai kas rada sekas vairāk nekā vienā dalībvalstī nolūkā saņemt atzinumu.

(2) EDAK atzinumu pieņem saskaņā ar VDAR 64. panta 3. punktu saistībā ar EDAK reglamenta 10. panta 2. punktu astoņu nedēļu laikā pēc tam, kad priekšsēdētājs un kompetentā UI ir pieņēmuši lēmumu, ka lieta ir pilnīga. Ņemot vērā jautājuma sarežģītību, ar priekšsēdētāja lēmumu šo laikposmu var pagarināt vēl par sešām nedēļām,

ir pieņēmusi šo atzinumu.

1 IEVADS

1.1 Faktu kopsavilkums

1. Francijas uzraudzības iestāde (turpmāk – **FR UI**) 2024. gada 16. februārī lūdza kolēģiju sniegt atzinumu par to, vai sejas atpazīšanas tehnoloģija, ko lidostu ekspluatanti un aviosabiedrības izmanto, lai ar biometrisku datu palīdzību autentificētu un identificētu pasažierus² nolūkā racionalizēt pasažieru plūsmu lidostas drošības kontrolpunktos³, bagāžas nodošanas punktos, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpām (izņemot robežkontroli un pārbaudes, ko veic beznodokļu veikali), sader ar VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu (turpmāk – **pieprasījums**). FR UI savam pieprasījumam pievienoja tipisku lietošanas gadījumu aprakstu (I pielikums).

¹ Atsauces uz jēdzienu “**dalībvalstis**” visā šajā atzinumā jāsaprot kā atsauces uz EEZ dalībvalstīm. Šajā atzinumā atsauces uz jēdzienu “Savienība” jeb “ES” jāsaprot kā atsauces uz EEZ.

² Šajā atzinumā “**pasažieris**” ir datu subjekts, kura personas dati tiek apstrādāti šajā atzinumā aprakstītajā konkrētajā nolūkā. Turpmāk šajā atzinumā termini “pasažieris” un “persona” tiek lietoti kā savstarpēji aizstājami termini.

³ Šajā atzinumā jēdziens “**lidostas drošības kontrolpunkti**” ir saistīts ar drošības pārbaudēm, kuras veic, lidostas ekspluatantam par to uzņemoties atbildību, un kuras pasažieriem jāveic, lai no izlidošanas zāles nonāktu iekāpšanas zonā vai pie iekāpšanas vārtiem.

2. Savā pieprasījumā FR UI norāda, ka modeļi, kas pašlaik tiek testēti vairākās ES lidostās, dažādās dalībvalstīs atšķiras, tādējādi, iespējams, radot risku, ka uzraudzības iestāžu interpretācijas atšķiras, kā arī risku, ka tiks radīta atšķirīga ietekme uz datu subjektu pamattiesībām un brīvībām ES⁴.
3. Kolēģija uzskata, ka, lai sniegtu atbildi uz FR UI pieprasījumu, ir jāatbild uz turpmāk norādītajiem jautājumiem.

4. **1. jautājums.**

1.1. Vai sejas atpazīšanas tehnoloģijas izmantošana autentifikācijai, izmantojot biometriskus datus, **lai racionalizētu pasažieru plūsmu lidostās** (drošības kontrolpunkti, bagāžas nodošanas punkti, iekāpšanas laikā un pieklūstot pasažieru atpūtas telpai), ir saderīga ar **VDAR 5. panta 1. punkta f) apakšpunktu, 25. un 32. pantu** tādas glabāšanas arhitektūras gadījumā, kurā katra pasažiera biometrisko veidni glabā tikai **attiecīgais pasažieris**, piemēram, lokāli savā individuālajā ierīcē, kas atrodas tikai viņa kontrolē?

1.2. Ja šāda apstrāde tiktu atzīta par saderīgu ar iepriekš minētajiem noteikumiem, kādas minimālās garantijas būtu vajadzīgas, ņemot vērā VDAR 25. un 32. pantu?

2. jautājums.

2.1. Vai sejas atpazīšanas tehnoloģijas izmantošana autentifikācijai vai identifikācijai, izmantojot biometriskus datus, **lai racionalizētu pasažieru plūsmu lidostās** (drošības kontrolpunkti, bagāžas nodošanas punkti, iekāpšanas laikā un pieklūstot pasažieru atpūtas telpai), ir saderīga ar **VDAR 5. panta 1. punkta e) un f) apakšpunktu, 25. un 32. pantu centralizētas** glabāšanas arhitektūras gadījumā, ja visu pasažieru biometriskās veidnes glabā centralizētā datubāzē:

2.1.1. Lidostas centrālajā datubāzē, ko kontrolē lidostas ekspluatants, šifrētā veidā, ar atslēgu / slepenu paroli, kas atrodas tikai pie attiecīgās personas (piemēram, personas mobilajā tālrunī), lai veiktu autentifikāciju?

2.1.2. Ja šāda apstrāde tiktu atzīta par saderīgu, kādas minimālās, pienācīgās garantijas būtu vajadzīgas, ņemot vērā VDAR 25. un 32. pantu?

2.2.1. Lidostas centrālajā datubāzē, ko kontrolē lidostas ekspluatants, šifrētā veidā, ar atslēgām, kas ir lidostas ekspluatanta rīcībā, lai veiktu identifikāciju?

2.2.2. Ja šāda apstrāde tiktu atzīta par saderīgu, kādas minimālās, pienācīgās garantijas būtu vajadzīgas, ņemot vērā VDAR 25. un 32. pantu?

2.3.1. Mākonī, aviosabiedrības vai tās pakalpojumu sniedzēja (apstrādātāja) kontrolē, šifrētā veidā, ar atslēgām, kas ir aviosabiedrības vai tās pakalpojumu sniedzēja rīcībā, lai veiktu identifikāciju?

⁴ Pieprasījuma 1. punkts.

2.3.2. Ja šāda apstrāde tiktu atzīta par saderīgu, kādas minimālās, pienācīgās garantijas būtu vajadzīgas, ņemot vērā VDAR 25. un 32. pantu?

5. Pēc tam, kad FR UI 2024. gada 16. februārī atzina lietu par pilnīgu un kolēģijas priekšsēdētāja 2024. gada 23. februārī atzina lietu par pilnīgu, sekretariāts to izplatīja 2024. gada 23. februārī. Ievērojot VDAR 64. panta 3. punktu un skatot to kopā ar EDAK reglamenta 10. panta 2. punktu, EDAK priekšsēdētāja jautājuma sarežģītības dēļ nolēma pagarināt parasto termiņu, kas ir astoņas nedēļas, par vēl sešām nedēļām.

1.2 Pieprasījuma sniegt atzinumu saskaņā ar VDAR 64. panta 2. punktu pieņemamība

6. VDAR 64. panta 2. punktā ir noteikts, ka jebkura uzraudzības iestāde var pieprasīt, lai kolēģija izskata jebkuru jautājumu par vispārējo piemērošanu vai kas rada sekas vairāk nekā vienā dalībvalstī nolūkā saņemt atzinumu.
7. Kolēģija uzskata, ka FR UI iesniegtais pieprasījums par sejas atpazīšanas tehnoloģijas izmantošanas atbilstību, lai veiktu autentificēšanu vai identifikāciju, izmantojot biometriskus datus, ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās attiecas uz jautājumiem, kas "rada sekas vairāk nekā vienā dalībvalstī", jo, kā paskaidrots pieprasījumā⁵, pašlaik dalībvalstu lidostās tiek īstenoti vairāki projekti un tiek lēsts, ka turpmākajos gados šāda izmantošana kļūs plašāka. Modeļi, kurus pašlaik testē dažādās lidostas un aviosabiedrības, dažādās dalībvalstīs ievērojami atšķiras, tā iespējami radot risku, ka datu aizsardzības ziņā vairāk nekā vienā dalībvalstī būs atšķirīga ietekme.
8. Kolēģija arī uzskata, ka FR UI iesniegtais pieprasījums būtiski ietekmē VDAR 5. panta 1. punkta e) un f) apakšpunktā noteikto principu piemērošanu un saskaņā ar VDAR 25. pantu pārziņiem piemērojamās prasības, kā arī saskaņā ar VDAR 32. pantu pārziņiem un apstrādātājiem piemērojamās prasības. Tāpēc šis pieprasījums ir saistīts ar "jautājumu par vispārējo piemērošanu" VDAR 64. panta 2. punkta nozīmē, jo tas attiecas uz glabāšanas ierobežojuma (VDAR 5. panta 1. punkta e) apakšpunkts) un integritātes un konfidencialitātes (VDAR 5. panta 1. punkta f) apakšpunkts) principu konsekventu interpretāciju, kā arī integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma jēdzienu (VDAR 25. pants) un datu drošības jēdzienu (VDAR 32. pants), lai cita starpā nodrošinātu minēto noteikumu konsekventu piemērošanu EEZ.
9. Visas iespējamās atšķirīgās nostājas dalībvalstīs attiecībā uz VDAR 5. panta 1. punkta e) un f) apakšpunkta un 25. un 32. panta interpretāciju palielinātu risku, ka lidostu ekspluatanti un aviosabiedrības varētu izstrādāt sejas atpazīšanas projektus nekonekventi. Tā kā FR UI ir skaidri pierādījusi, ka šie noteikumi ir konsekventi jāinterpretē attiecībā uz sejas atpazīšanas tehnoloģijas izmantošanu, lai ar biometrisku datu palīdzību autentificētu vai identificētu pasažierus nolūkā racionalizēt pasažieru plūsmu lidostās⁶, kolēģija uzskata, ka pieprasījums ir pamatots atbilstoši EDAK reglamenta 10. panta 3. punktam.
10. Saskaņā ar VDAR 64. panta 3. punktu EDAK nesniedz atzinumu, ja tā jau ir sniegusi atzinumu par attiecīgo jautājumu⁷. EDAK vēl nav sniegusi atbildes uz jautājumiem, kas izriet no šā pieprasījuma. Lai

⁵ Pieprasījuma 3. punkts.

⁶ Pieprasījuma 1.–3. punkts.

⁷ VDAR 64. panta 3. punkts un EDAK reglamenta 10. panta 4. punkts.

gan EDAK Pamatnostādnēs 3/2019 par videoierīcēm⁸ jau ir iekļauti daži noderīgi elementi, kas attiecas uz drošības pasākumiem, kas būtu jāpiemēro biometrisku datu apstrādei, tajās nav aplūkoti visi aspekti, kas saistīti ar pieprasījumā uzdotajiem jautājumiem. Turklāt pieejamajos EDAK norādījumos, tostarp EDAK Pamatnostādnēs 3/2019 par videoierīcēm, nav sniegti konkrēti norādījumi par iespējamiem elementiem, kas jāpārbauda saistībā ar biometrisku datu centralizētu vai decentralizētu glabāšanu, lai veiktu pasažieru identificēšanu vai autentificēšanu, nolūkā racionalizēt pasažieru plūsmu lidostās, un par šādas apstrādes saderību ar VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu.

11. Šo iemeslu dēļ kolēģija uzskata, ka pieprasījums ir pieņemams un ka tajā uzdotie jautājumi būtu jāanalizē atzinumā, kas pieņemts saskaņā ar VDAR 64. panta 2. punktu.

2 ATZINUMA DARBĪBAS JOMA UN KONTEKSTS

2.1 Atzinuma darbības joma

12. Šis atzinums attiecas tikai uz to, vai lidostas ekspluatantu un aviosabiedrību veiktā sejas atpazīšanas tehnoloģijas izmantošana, lai autentificētu vai identificētu pasažierus, izmantojot biometriskos datus, **ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās**, proti, drošības kontrolpunktos, bagāžas nodošanas punktos, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpai, kā norādīts pieprasījumā, ir saderīga ar VDAR 5. panta 1. punkta e) un f) apakšpunktu, kā arī 25. un 32. pantu.

13. Attiecībā uz **šā atzinuma darbības jomu** kolēģija precizē:

- 1) šis atzinums neattiecas uz personas datu apstrādi saistībā ar robežkontroli un kontroli, ko veic beznodokļu veikali, jo to veic pārzīņi, kas nav lidostu ekspluatanti un aviosabiedrības;
- 2) sejas atpazīšanas tehnoloģijas izmantošana jebkādiem citiem mērķiem (piemēram, tiesībaizsardzībai) nav šā atzinuma darbības jomā pat tad, ja tā ir balstīta uz 3.2. iedaļā aprakstītajiem scenārijiem. Tas pats attiecas uz šīs tehnoloģijas izmantošanu, ko veic jebkura cita persona, pat ja tā paredzēta līdzīgiem mērķiem;
- 3) šajā atzinumā ir aplūkota tikai pasažieru personas datu apstrāde, un tas neattiecas uz cita veida datu subjektiem, piemēram, lidostu ekspluatantu vai aviosabiedrību darbiniekiem;
- 4) šajā atzinumā ir izskatīts FR UI iesniegtais pieprasījums attiecībā uz pasažieru biometrisku veidņu glabāšanas arhitektūras saderību ar VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu. Šajā sakarā šajā atzinumā nav iekļauta pilnīga analīze par to, kā katrā atsevišķā gadījumā attiecīgais(-ie) pārzinis(-ņi), kā arī attiecīgā gadījumā tā/to apstrādātājs(-i) ievēro VDAR. Tas ir īpaši svarīgi, ņemot vērā, ka šīs tehnoloģijas rada paaugstinātu risku, kas saistīts ar īpašu kategoriju datu apstrādi saskaņā ar VDAR 9. pantu. Tāpēc šis atzinums neskar novērtējumu par citiem VDAR

⁸ EDAK Pamatnostādnes 3/2019 par personas datu apstrādi, izmantojot videoierīces, Versija 2.0, pieņemtas 2020. gada 29. janvārī (turpmāk – **EDAK Pamatnostādnes 3/2019 par videoierīcēm**).

noteikumiem attiecībā uz sejas atpazīšanas tehnoloģiju izmantošanu, tostarp konkrētajā nozarē, uz kuru attiecas pieprasījums, vai atsevišķu gadījumu juridisko un tehnisko analīzi, kuras pamatā ir pārziņa paredzētā konkrētā apstrāde un apstākļi;

- 5) šajā atzinumā nav aplūkota bērnu personas datu apstrāde, un tas neskar nekādas īpašās prasības, kas šajā ziņā ir piemērojamas;
 - 6) šis atzinums neskar juridiskās prasības un turpmākus biometrisko datu izmantošanas ierobežojumus, kas izriet no dalībvalstu tiesību aktiem⁹;
 - 7) šajā atzinumā izdarītie secinājumi neskar tehnoloģiju turpmāku attīstību;
 - 8) šajā atzinumā aplūkoti četri scenāriji, kuru specifiskās iezīmes ir aprakstītas 3.2. iedaļā. Tas neattiecas uz citiem scenārijiem, pat ja apstrādi veic tādos pašos nolūkos.
14. Savā pieprasījumā FR UI norādīja, ka pasažieru biometrisko datu apstrāde nolūkā racionalizēt pasažieru plūsmu lidostās būtu balstīta uz pieņēmumu, ka personas piekriņš šādai apstrādei, kas, iespējams, kļūtu par juridisko pamatu saskaņā ar VDAR¹⁰. **Tomēr piemērojamā juridiskā pamata analīze nav to jautājumu lokā, kas EDAK uzdoti pieprasījumā, un līdz ar to piekrišanas šādai apstrādei spēkā esamība saskaņā ar VDAR 6., 7. un 9. pantu šajā atzinumā nav izvērtēta.**
15. Tomēr EDAK vispārīgi norāda, ka tad, ja attiecīgie pārziņi izmantotu šo juridisko pamatu, tiem no personām, kas vēlas izmantot šādus pakalpojumus, būtu jāsaņem derīga un nepārprotama piekrišana¹¹. Šādai nepārprotamai piekrišanai vajadzētu būt brīvi sniegtai, konkrētai un apzinātai¹², un šo nosacījumu izpilde tiktu analizēta katrā atsevišķā gadījumā. Tas cita starpā nozīmē, ka:
- 1) personām būtu jāspēj jebkurā laikā un bez jebkādām nelabvēlīgām sekām viegli atsaukt šādu piekrišanu¹³;
 - 2) lai piekrišana būtu brīvi sniegta, šāda biometrisko datu tehnoloģiju izmantošana var notikt tikai brīvprātīgi, jo personām vajadzētu būt iespējai brīvi izvēlēties, vai izmantot šos pakalpojumus, bez jebkādām nelabvēlīgām sekām (piemēram, ievērojami

⁹ Piemēram, VDAR 9. panta 4. punktā ir noteikts, ka dalībvalstis var saglabāt vai ieviest papildu nosacījumus, tostarp ierobežojumus, attiecībā uz biometrisko datu apstrādi.

¹⁰ Pieprasījuma I pielikums.

¹¹ Saskaņā ar VDAR 4. panta 14. punktu un 9. panta 1. punktu, kā arī VDAR 9. panta 2. punkta a) apakšpunktu biometrisko datu apstrāde fiziskas personas unikālas identifikācijas nolūkā ir aizliegta, ja vien datu subjekts nav devis nepārprotamu piekrišanu minēto personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, izņemot gadījumus, kad Savienības vai dalībvalsts tiesību aktos ir paredzēts, ka datu subjekts nevar atcelt VDAR 9. panta 1. punktā minēto aizliegumu. Sk. arī VDAR 51., 52. un 53. apsvērumu.

¹² VDAR 4. panta 11. punkts un 7. pants.

¹³ VDAR 7. panta 4. punkts, arī VDAR 50. apsvērumus.

ilgākiem kavējumiem pasažieriem, kuri nepiekrīt¹⁴), stimuliem, papildu izmaksām vai papildu priekšrocībām¹⁵;

- 3) nepārprotama piekrišana būtu arī jāsaņem no personām, kuru biometriskie dati tiek apstrādāti, pat ja tās nav pieteikušās, lai tās tiktu identificētas vai autentificētas ar šādiem līdzekļiem. Citiem vārdiem sakot, ir būtiski, lai to personu sejas, kuras nav nepārprotami piekritušas sejas atpazīšanai paredzētajam nolūkam, netiktu skenētas ar kamerām. To var panākt, piemēram, atvēlot īpašas joslas sejas atpazīšanai un nodrošinot atbilstošas norādes un fizisku nošķiršanu no plūsmām bez biometriskas kontroles, lai šādas joslas varētu skaidri identificēt;
 - 4) neskarot to, vai šādai apstrādei piemērojama juridiskais pamats būtu piekrišana, VDAR 5. pantā noteiktie apstrādes principi attiecībā uz nepieciešamību un proporcionalitāti joprojām ir piemērojami pat tad, ja personas ir devušas nepārprotamu piekrišanu savu biometrisku datu izmantošanai¹⁶.
16. Pieprasījumā ir precizēts¹⁷, ka lidostu ekspluatanti darbotos kā pārziņi attiecībā uz apstrādi lidostas drošības kontrolpunktos, bet aviosabiedrības darbotos kā pārziņi attiecībā uz apstrādi bagāžas nodošanas punktos, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpām. Tāpēc kolēģija norāda, ka pieprasījumā aprakstītajā apstrādē varētu būt iesaistīti dažādi dalībnieki un ka tā nav novērtējusi (kopīgā) pārziņa un apstrādātāja lomu īstenošanu šā atzinuma 3.2. iedaļā izklāstītajos scenārijos. Katrā gadījumā jānosaka iesaistītie dalībnieki un skaidri jāsadala to pienākumi, lai tiktu ievērotas VDAR prasības¹⁸.
17. Kolēģija arī norāda, ka pašlaik ES nav vienotas juridiskas prasības lidostu ekspluatantiem un aviosabiedrībām identificēt pasažierus un visos iepriekš minētajos kontrolpunktos pārbaudīt, vai vārds un uzvārds pasažiera iekāpšanas kartē atbilst personu apliecinošajā dokumentā norādītajam vārdam un uzvārdam¹⁹. Tādējādi uz visām šādām prasībām attiecas valsts tiesību akti, kas dažādās dalībvalstīs var atšķirties. Dažās dalībvalstīs šāda pārbaude var būt nepieciešama dažos kontrolpunktos (piemēram, bagāžas nodošanas vai iekāpšanas vietā), savukārt citās dalībvalstīs šādas pārbaudes

¹⁴ Piemēram, tas varētu ietvert tādus apsvērumus kā sistēmas izstrāde, lai izvairītos no sociālā spiediena uz pasažieriem, kuri nevēlas dot piekrišanu, izvairoties no tā, ka tās izvēle negatīvi ietekmē citus pasažierus.

¹⁵ EDAK Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, Versija 1.1, pieņemtas 2020. gada 4. maijā (turpmāk – **EDAK Pamatnostādnes 5/2020 par piekrišanu**), 46. un 48. punkts.

¹⁶ Turpat, 5. punkts.

¹⁷ Pieprasījuma I pielikums.

¹⁸ Saskaņā ar VDAR 4. panta 7. un 8. punktu, 5. panta 2. punktu, 24., 26., 28. un 29. pantu. Skatīt arī EDAK Pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR, Versija 2.1, pieņemtas 2021. gada 7. jūlijā.

¹⁹ Attiecīgā regula ES līmenī ir Komisijas 2015. gada 5. novembra Īstenošanas regula (ES) 2015/1998, ar ko nosaka sīki izstrādātus pasākumus kopīgu pamatstandartu īstenošanai aviācijas drošības jomā. Tomēr šī regula neattiecas uz oficiālo personu apliecinošu dokumentu pārbaudēm lidostu kontrolpunktos, un dalībvalstīm ir rīcības brīvība to reglamentēt valsts līmenī.

pašlaik nav vajadzīgas²⁰. Juridisku pienākumu pārbaudīt pasažieru identitāti esība tieši ietekmē dažādu lidostu praksi.

18. Līdz ar to šajās situācijās, kad nav nepieciešama pasažieru identitātes pārbaude, salīdzinot ar oficiālu personu apliecinošu dokumentu, nebūtu jāveic pārbaude, izmantojot biometriskos datus, jo tā rezultātā datu apstrāde būtu pārmērīga, jo salīdzinājumā ar pašreizējo situāciju tas nozīmētu papildu datu apstrādi un tā būtu plašāka par to, kas nepieciešama attiecīgajā nolūkā, tādējādi neievērojot VDAR 5. panta 1. punkta c) apakšpunktā noteikto datu minimizēšanas principu. Šāds apsvērums jāņem vērā, izvērtējot visus šā atzinuma 3.2. iedaļā aprakstītos scenārijus.

2.2 Galvenie jēdzieni

19. Lai izejas datus varētu uzskatīt par biometriskiem datiem saskaņā ar VDAR 4. panta 14. punktu²¹, izejas datu, piemēram, fiziskas personas fizisko, fizioloģisko vai uzvedības pazīmju, apstrādei jābūt saistītai ar šo iezīmju mērījumiem, jo biometriskie dati ir šādu mērījumu rezultāts²².
20. Izmantojot personas sejas attēlu (fotogrāfiju vai video), ko sauc par biometrisko “**paraugu**”, ir iespējams iegūt šīs sejas atšķirīgo īpašību digitālu atveidojumu (to sauc par “**veidni**”)²³. Turklāt kolēģija atgādina, ka “[b]iometriskā veidne ir no biometriskā parauga iegūto unikālo iezīmju digitāls attēlojums, kuru var saglabāt biometriskajā datubāzē”²⁴, kas ļauj veikt fiziskas personas unikālo identifikāciju vai apstiprina to. Turklāt “[š]ai veidnei vajadzētu būt unikālai un specifiskai katrai personai, un principā tā ir pastāvīga laika gaitā”²⁵. Parasti salīdzināšanas procesā, kura mērķis ir identificēt vai autentificēt personu, izmantojot sejas atpazīšanu, saņemtu biometrisko veidni salīdzina ar glabātajiem datiem, lai pārbaudītu sakritību vai atrastu to datubāzē²⁶.

²⁰ Tas nozīmē, ka pašlaik vai nu vispār netiek veikta pārbaude, vai arī tiek pārbaudīta tikai iekāpšanas kartes esība. Piemēram, pamatojoties uz 1954. gada 22. maija Protokolu par Dānijas, Somijas, Norvēģijas un Zviedrijas valstspiederīgo atbrīvošanu no pienākuma uzrādīt pasi vai saņemt uzturēšanās atļauju, dzīvojot Skandināvijas valstī, kas nav viņu valsts, sākot no 1954. gada 1. jūlija, Norvēģijas, Dānijas, Somijas un Zviedrijas valstspiederīgie, ceļojot no vienas šīs valsts uz citu, ir atbrīvoti no pienākuma ņemt līdzi pasi vai citu ceļošanas identifikācijas dokumentu.

²¹ Sk. arī VDAR 51., 52. un 53. apsvērumu.

²² EDAK Pamatnostādnes 3/2019 par personas datu apstrādi, izmantojot videoierīces, 74. punkts.

²³ EDAK Pamatnostādnes 05/2022 par sejas atpazīšanas tehnoloģiju izmantošanu tiesībaizsardzības jomā, Versija 2.0, pieņemtas 2023. gada 26. aprīlī (turpmāk – **EDAK pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā**), 7. un 8. punkts.

²⁴ Turpat, 9. punkts.

²⁵ Turpat.

²⁶ EDAK Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 10.–11. punkts; sk. arī starptautisko standartu ISO/IEC 2382–37, 2022–03, pieejams: [https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022\(E\).zip](https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip) [pēdējo reizi skatīts 2024. gada 23. maijā]_(turpmāk – **ISO/IEC 2382-37**).

21. Sejas atpazīšanas tehnoloģijai var būt divas atšķirīgas funkcijas – autentifikācija²⁷ un identifikācija²⁸. Lai gan abas funkcijas ir atšķirīgas, abās izmanto biometrisko datu apstrādi, kas saistīta ar identificētu vai identificējamu fizisku personu²⁹, un tāpēc tās ir īpašu kategoriju personas datu apstrāde atbilstoši VDAR 9. pantam³⁰.
22. Proti:
- autentifikācijas** mērķis ir apstiprināt biometrisko identitāti, veicot salīdzināšanu. To sauc arī par pārbaudi “viens pret vienu”;
- identifikācijas** mērķis ir veikt meklēšanu biometriskās reģistrācijas datubāzē, lai atgrieztu identifikatorus, kas attiecināmi uz vienu personu. To sauc arī par identifikāciju “viens pret daudziem”.
23. Abos gadījumos (t. i., identifikācijas un autentifikācijas) lietotās sejas atpazīšanas metodes ir balstītas uz aplēsto atbilstību starp veidnēm, proti, salīdzināto veidni un pamatscenāriju(-iem). No šāda viedokļa tie ir iespējami: salīdzinājums rada lielāku vai mazāku varbūtību, ka persona patiešām ir autentificējamā vai identificējamā persona; ja šī varbūtība sistēmā pārsniedz noteiktu robežvērtību, ko noteicis sistēmas lietotājs vai izstrādātājs, sistēma pieņem, ka pastāv identificējama vai autentificējama atbilstība³¹.

²⁷ Kolēģija norāda, ka gaidāmās Eiropas Parlamenta un Padomes regulas, kas saskaņotas normas mākslīgā intelekta jomā, (Mākslīgā intelekta akts) (*Oficiālajā Vēstnesī* vēl nav publicēta) 3. panta 36. punktā “biometriskā verifikācija” arī ir definēta kā “automatizēta fizisku personu identitātes verifikācija “viens pret vienu”, tostarp autentifikācija, kas notiek, fiziskas personas biometriskos datus salīdzinot ar iepriekš sniegtiem biometriskajiem datiem” (sk. Eiropas Parlamenta 2024. gada 13. marta normatīvo rezolūciju par priekšlikumu Eiropas Parlamenta un Padomes regulai, kas saskaņotas normas mākslīgā intelekta jomā (Mākslīgā intelekta akts) un groza dažus Savienības leģislatīvos aktus (COM(2021)0206 – C9–0146/2021 – 2021/0106(COD))).

²⁸ Turpat, Mākslīgā intelekta akta 3. panta 35. punktā “biometriskā identifikācija” ir definēta kā “cilvēka fizisko, fizioloģisko, uzvedības vai psiholoģisko īpašību automatizēta atpazīšana nolūkā noskaidrot fiziskas personas identitāti, salīdzinot minētā indivīda biometriskos datus ar datubāzē glabātiem indivīdu biometriskajiem datiem”.

²⁹ ISO/IEC 2382-37.

³⁰ VDAR 4. panta 14. punkts un EDAK Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 12. punkts.

³¹ EDAK Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 11. punkts. Sk. arī ISO/IEC 2382-37.

3 PAR PIEPRASĪJUMA PAMATOTĪBU

3.1 Vispārējas piezīmes

24. Šajā sadaļā ir analizēti 4. punktā norādītie jautājumi. Šajā kontekstā attiecībā uz 1. jautājumu kolēģija analizēs saderību ar VDAR 5. panta 1. punkta f) apakšpunktu un 25. un 32. pantu, bet attiecībā uz 2. jautājumu – saderību ar VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu.
25. Šajā nolūkā kolēģija analizēs četrus dažādus scenārijus³², kuru specifiskās iezīmes ir aprakstītas turpmāk 3.2. iedaļā.
26. Vispirms kolēģija atgādina, ka biometrisko datu un jo īpaši sejas atpazīšanas tehnoloģijas izmantošana nozīmē paaugstinātu risku datu subjektu tiesībām un brīvībām. Pirmkārt, šāda apstrāde attiecas uz biometriskiem datiem, kam saskaņā ar VDAR 9. pantu ir piešķirta īpaša aizsardzība. Biometriskie dati neatgriezeniski maina cilvēka ķermeņa un identitātes attiecības, jo padara ķermeņa īpašības “mašīnlasāmas” un turpmāk izmantojamas³³. Turklāt sejas atpazīšanas tehnoloģijas izmantošana var radīt risku, kas saistīts ar pseidonegatīviem rezultātiem, neobjektivitāti un diskrimināciju³⁴, un iespējamā biometrisko datu ļaunprātīga izmantošana varētu radīt smagas sekas personām, piemēram, identitātes viltošanu vai izlikšanos par citu personu³⁵. Būtu arī jānorāda, ka gadījumos, kad sejas atpazīšana tiek veikta attālināti un bez aktīvas datu subjekta iesaistes, personas varētu būt vēl mazāk informētas par šādu apstrādi un par ar to saistīto risku. Visbeidzot, ir svarīgi uzsvērt, ka īpašības, uz kurām balstīti biometriskie dati, kopumā var uzskatīt par pastāvīgām un ka tās būtu jāuzskata par neatsaucamām, jo īpaši sejas atpazīšanas kontekstā³⁶.
27. Tāpēc, ņemot vērā iepriekš norādīto, pat ja šādas tehnoloģijas tiktu uzskatītas par īpaši efektīvām, pirms to izmantošanas pārziņiem būtu jānovērtē ietekme uz datu subjektu pamattiesībām un brīvībām un jāapsver, vai apstrādes leģitīmo nolūku var īstenot ar mazāk ierobežojošiem līdzekļiem³⁷.

³² Četri scenāriji, ko analizēja kolēģija, ir balstīti uz pieprasījuma I pielikumā norādītajiem lietošanas gadījumiem. FR UI ir precizējusi, ka pieprasījuma I pielikumā izklāstītie lietošanas gadījumi ir īstenošanas piemēri, kas ir daļa no scenārija un ko izmanto ilustratīvos nolūkos.

³³ 29. panta darba grupas Atzinums 3/2012 par biometrijas tehnoloģiju attīstību, pieņemts 2012. gada 27. aprīlī, WP193 (turpmāk – **29. panta darba grupas Atzinums 3/2012 par biometrijas tehnoloģijām**), 4. lpp. Jānorāda, ka šajā atzinumā ir atsauce uz 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Datu aizsardzības direktīva). VDAR ir paplašinājusi īpašu kategoriju datu tvērumu, un atšķirībā no Datu aizsardzības direktīvas VDAR ir noteikts, ka biometriskie dati ir īpašu kategoriju dati (VDAR 9. pants).

³⁴ Pamatnostādnes par sejas atpazīšanu, Eiropas Padomes Konvencijas par personu aizsardzību attiecībā uz personas datu automatisko apstrādi konsultatīvā komiteja, 2021. gada jūnijs, 15. lpp.; arī EDAK Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 27. punkts.

³⁵ 29. panta darba grupas Atzinums 3/2012 par biometrijas tehnoloģiju attīstību, 29. lpp.

³⁶ EDAK Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 104. punkts.

³⁷ VDAR 39. apsvēruma. Sk. arī EDAK Pamatnostādnes 3/2019 par videoierīcēm, 73. punkts.

28. Kolēģija arī atgādina, ka tiesības uz personas datu aizsardzību nav absolūtas un ka tās būtu jālīdzsvaro ar citām pamattiesībām, ko aizsargā Harta, saskaņā ar proporcionalitātes principu³⁸.
29. VDAR 25. panta 1. punktā ir atsauce uz “datu aizsardzības principiem”, kas uzskaitīti VDAR 5. pantā³⁹, un noteikts, ka tie integrēti jāīsteno “efektīvi”⁴⁰. Tas nepārprotami ietver datu minimizēšanas principu saskaņā ar VDAR 5. panta 1. punkta c) apakšpunktu⁴¹, kurā noteikts, ka personas dati ir “adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos, un kurš atspoguļo minēto samērīguma principu”⁴². Turklāt VDAR 25. panta 2. punktā ir precizēts “datu minimizēšanas pēc noklusējuma” pienākums, norādot, ka tas attiecas uz savākto personas datu apjomu, to apstrādes apmēru, glabāšanas ilgumu un to pieejamību⁴³.
30. Tomēr VDAR 25. pantā nav noteikts, ka pārziņiem ir jāīsteno kādi konkrēti tehniski un organizatoriski pasākumi, bet gan prasīts, lai izvēlētie pasākumi un garantijas atbilstu kontekstam un riskam, ko datu subjekta tiesībām un brīvībām rada apstrāde⁴⁴. Tāpat VDAR 32. pantā par apstrādes drošību ir noteikts, ka pārziņiem un apstrādātājiem ir jāīsteno atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam attiecībā uz fizisku personu tiesībām un brīvībām.

³⁸ VDAR 4. apsvērums. Šajā sakarā skatīt arī Tiesas 2021. gada 22. jūnija sprieduma lietā *Latvijas Republikas Saeima, C-439/19*, ECLI:EU:C:2021:504 (turpmāk – lieta C-439/19 *Latvijas Republikas Saeima*), 98., 110. un 113. punktu. Turklāt saskaņā ar proporcionalitātes principu kā vispārēju Savienības tiesību principu ar Savienības tiesību aktiem ieviestajiem pasākumiem ir jābūt piemērotiem vēlamā mērķa sasniegšanai un tie nedrīkst pārsniegt to, kas ir nepieciešams šā mērķa sasniegšanai (sk. Tiesas 2010. gada 9. novembra sprieduma lietā *Volker und Markus Schecke and Eifert, C-92/09 un C-93/09*, ECLI:EU:C:2010:662 (turpmāk tekstā – C-92/09 un C-93/09 *Volker und Schecke*) 74. punktu un tajā minēto judikatūru).

³⁹ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, Versija 2.0, pieņemtas 2020. gada 20. oktobrī (turpmāk – **EDAK Pamatnostādnes 4/2019 par integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma**), 11. punkts.

⁴⁰ VDAR 25. panta 1. punktā ir noteikts: “Ņemot vērā progresa līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, kurus rada apstrāde, pārzinis gan apstrādes līdzekļu noteikšanas, gan pašas apstrādes laikā īsteno atbilstošus tehniskus un organizatoriskus pasākumus, piemēram, pseidonimizāciju, kas ir paredzēti, lai efektīvi īstenotu datu aizsardzības principus, piemēram, datu minimizēšanu, un lai apstrādē integrētu vajadzīgās garantijas nolūkā izpildīt šīs regulas prasības un aizsargāt datu subjektu tiesības.” Sk. arī EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 13. punkts.

⁴¹ Attiecīgi VDAR 39. apsvērumā ir noteikts, ka personas dati būtu jāapstrādā tikai tad, ja apstrādes nolūku nav iespējams pienācīgi sasniegt citiem līdzekļiem.

⁴² C-439/19 *Latvijas Republikas Saeima*, 98. punkts; Tiesas 2019. gada 11. decembra spriedums lietā *Asociaia de Proprietari bloc M5A-ScaraA, C-708/18*, ECLI:EU:C:2019:1064 (turpmāk – C-708/18 *M5A-ScaraA*), 48. punkts.

⁴³ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 48. punkts.

⁴⁴ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 14. punkts.

31. Svarīgi, ka pat tad, ja pasažieriem būtu nepārprotami jāpiekrīt savu biometrisko datu izmantošanai, lai racionalizētu pasažieru plūsmu lidostās, joprojām būtu piemērojami VDAR noteiktie apstrādes principi attiecībā uz nepieciešamību un proporcionalitāti, kas būtu jāievēro⁴⁵.
32. Attiecībā uz **nepieciešamības principu** kolēģija apsvērs, vai ierosinātā apstrāde ir nepieciešama, lai sasniegtu vēlamu mērķi, un vai to pašu mērķi tikpat efektīvi var sasniegt ar citiem līdzekļiem, kas mazāk ietekmē datu subjekta pamattiesības un brīvības⁴⁶. Attiecībā uz **proporcionalitātes principu** kolēģija novērtēs, vai negatīvā ietekme uz datu subjektu pamattiesībām un brīvībām ir samērīga ar jebkādu paredzamo ieguvumu. Ja ieguvums ir salīdzinoši neliels, šāda ietekme var būt nesamērīga⁴⁷.
33. Jebkurā gadījumā, pat ja kolēģija uzskata, ka kāds no turpmāk analizētajiem scenārijiem varētu atbilst VDAR 5. panta 1. punkta e) un f) apakšpunkta, 25. un 32. panta prasībām, pārzinim visos gadījumos tas ir jāpierāda ar faktiem. Šādā pierādījumā būtu jāapsver alternatīvi scenāriji.

3.2 Par saderību ar VDAR 5. panta 1. punkta e) un f) apakšpunktu, 25. un 32. pantu

3.2.1 1. scenārijs – reģistrētās biometriskās veidnes glabāšana tikai pie attiecīgās personas, lai veiktu autentifikāciju

34. Šajā iedaļā tiek pētīts, vai pasažieru biometriskās veidnes glabāšana autentifikācijas nolūkos tikai pie attiecīgās personas, piemēram, viņas individuālajā ierīcē⁴⁸, ko kontrolē tikai šī persona^{49,50} (turpmāk – **1. scenārijs**), sader ar VDAR 5. panta 1. punkta f) apakšpunktu un 25. un 32. pantu. Šajā iedaļā ir arī aplūkotas 1. scenārijam atbilstošas garantijas, ņemot vērā VDAR 25. un 32. pantu.

Scenārija apraksts

35. 1. scenārijā katra pasažiera, kurš piekritis šādai apstrādei, reģistrētā biometriskā veidne tiek glabāta tikai pie šīs personas, piemēram, individuālā ierīcē, kas atrodas pie šī pasažiera un ir pilnīgā viņa kontrolē. Pasažieri tiek autentificēti (tieša salīdzināšana), kad viņus pārbauda īpašos kontrolpunktos lidostā.
36. Lidostas ekspluatants reģistrāciju veic vai nu attālināti, izmantojot lidostas ekspluatanta lietotni⁵¹, vai arī lidostas termināļos, nodrošinot atbilstošu identitātes garantijas līmeni (piemēram, *eIDAS* atbilstošu

⁴⁵ EDAK Pamatnostādnes 5/2020 par piekrišanu saskaņā ar Regulu 2016/679, 5. punkts.

⁴⁶ C-439/19 *Latvijas Republikas Saeima*, 110. un 113. punkts; Tiesas (virspalāta) 2023. gada 4. jūlija spriedums lietā *Meta v. Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, 108. punkts.

⁴⁷ C-708/18 *M5A-ScaraA*, 52.–56. punkts, C-92/09 un C-93/09 *Volker und Schecke*, 87. punkts, C-439/19 *Latvijas Republikas Saeima*, 98., 110., 113. punkts. Sk. arī 29. panta darba grupas Atzinumu 3/2012 par biometrijas tehnoloģiju attīstību, 8. lpp.

⁴⁸ Kā alternatīvu persona varētu izdrukāt un glabāt savu biometrisko veidni papīra formātā.

⁴⁹ Tas neskar pārziņa vispārējo atbildību par apstrādi.

⁵⁰ Kā piemēru var minēt 1. izmantošanas gadījumu, kas aprakstīts pieprasījuma I pielikumā.

⁵¹ EDAK norāda, ka nākotnē varētu paredzēt alternatīvus šādas reģistrācijas veidus un reģistrāciju, iespējams, varētu veikt bez kādas konkrētas lidostas ekspluatanta lietotnes, piemēram, mijiedarbojoties ar lietotāja digitālo maku.

pārlicības līmeni⁵²). Šāda reģistrācija sastāv no biometriskās veidnes un identifikācijas datu⁵³ (turpmāk – **ID**), kas nepieciešami datu apstrādei, reģistrēšanas pasažiera ierīcē. Reģistrācija notiek tikai vienreiz un ir spēkā konkrētu derīguma periodu (piemēram, atbilstoši pasažieru pases derīguma termiņam). Pēc reģistrācijas procesa lidostas ekspluatants neglabā ne pasažieru identifikācijas, ne biometriskos datus.

37. Jo īpaši attiecībā uz glabāšanu pasažiera identifikācijas dati un biometriskā veidne tiek uzglabāti lokāli katra pasažiera ierīcē (piemēram, lidostas ekspluatanta mobilajā lietotnē vai digitālā maka lietotnē). Pēc tam ierīci var izmantot, lai pārsūtītu pasažieru identifikācijas datus un biometrisko veidni vai veiktu vaicājumu par tiem, iespējams, iekļaujot informāciju par lidojumu un/vai iekāpšanas karti. Piemēram, šī informācija ir šifrēta ar atslēgu, kas ir tikai lidostas ekspluatanta rīcībā – to var kodēt kā *QR* kodu, ko var izdrukāt uz papīra vai parādīt pasažiera ierīces ekrānā. Šajā gadījumā pasažieris parādītu šo *QR* kodu īpašā kontroles iekārtā lidostā, kas aprīkota ar *QR* skeneri un kameru.
38. Drošības ziņā atbilstības meklēšanas laikā *QR* kodus atšifrē ar atslēgu, kas atrodas pie lidostas ekspluatanta, kurš ir vienīgā persona, kas var atšifrēt *QR* kodus. Pasažieru biometriskos datus glabā tikai ļoti īsu laiku un dzēš pēc atbilstības meklēšanas pabeigšanas. Jānorāda, ka ar glabāšanu saistītie drošības pasākumi daļēji ir atkarīgi no pasažiera ierīces drošības.

EDAK novērtējums

39. 1. scenārijā aprakstīti tehniskie un organizatoriskie pasākumi, kas paredzēti, lai nodrošinātu tādu drošības līmeni, kas atbilst datu subjektiem radītajam riskam, kā noteikts VDAR 5. panta 1. punkta f) apakšpunktā un 32. pantā. Pasažieri tiek autentificēti (tieša salīdzināšana), kad viņus pārbauda īpašos kontrolpunktos lidostā. Šajā scenārijā galvenā atbilstības meklēšanas darbība tiek veikta kontrolētas vides kontekstā⁵⁴, kurā pasažieri aktīvi iesaistās un kurā pasažieriem ir lielāka kontrole pār saviem datiem. Jo īpaši tiktu pārbaudīti tikai tie pasažieri, kuri ir piekrituši šādai apstrādei, un, tā kā pārbaude tiktu veikta īpašās iekārtās, netiktu vākti citu tādu pasažieru biometriskie dati, kuri nepiekrita šādai apstrādei. Turklāt pasažieriem, kuri dod piekrišanu, ir iespēja jebkurā brīdī pārtraukt apstrādi, dzēšot datus no savas ierīces.
40. Sejas atpazīšanas tehnoloģijas izmantošana, pamatojoties tikai uz personas glabātu biometrisko veidni, kas, piemēram, var būt pasažierim piederošā individuālā ierīcē, ko kontrolē tikai pasažieris un ko izmanto autentifikācijai īpašos kontrolpunktos caur specializētu saskarni, noteiktos apstākļos rada mazāku risku salīdzinājumā ar biometrisko datu izmantošanu, ja dati tiek glabāti centralizētā

⁵² Elektroniskās identifikācijas un uzticamības pakalpojumu satvars (turpmāk – **eIDAS**), pamatojoties uz Eiropas Parlamenta un Padomes 2024. gada 11. aprīļa Regulu (ES) 2024/1183, ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi.

⁵³ Šajā atzinumā identifikācijas dati ir tādi dati kā uzvārds, vārds, dzimšanas datums utt., kas ir pārbaudīti un atzīti par pareiziem attiecībā uz personu apliecinošu dokumentu vai pasi.

⁵⁴ “Nekontrolēta vide” nozīmē sejas atpazīšanas tehnoloģijas izmantošanu identifikācijai bez datu subjektu aktīvas iesaistīšanās, kur katras sejas veidne, kas iekļūst uzraudzības zonā, tiek salīdzināta ar veidnēm no plaša populācijas šķērsgriezuma, kas glabājas datubāzē; sk. EDAK Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 17. punkts.

datubāzē⁵⁵. Šāda lokalizēta glabāšana, kad to papildina atbilstošas garantijas⁵⁶, skarto personu skaita ziņā samazina personas datu aizsardzības pārkāpumu smaguma pakāpi salīdzinājumā ar centralizētu glabāšanu un nodrošina, ka piekļuve biometriskajai veidnei ietver datu subjekta aktīvu iesaisti.

41. Turklāt atbilstības meklēšanu varētu veikt uz vietas lidostā, salīdzinot biometrisko veidni, piemēram, QR kodā, ar veidnes izvaddatiem, kas aprēķināti, izmantojot ar kontroles iekārtas kameru uzvertu biometrisko paraugu. Pārbaudītājam, kurš veic īpašu pārbaudi (kas varētu būt lidostas ekspluatants vai aviosabiedrība atkarībā no tā, vai pārbaude tiek veikta lidostas drošības kontrolpunktos, bagāžas nodošanas punktos, iekāpšanas laikā un/vai piekļūstot pasažieru atpūtas telpai), tiktu darīts zināms un tas izmantotu tikai atbilstošo rezultātu. Turklāt tas, ka atbilstības meklēšanai nepieciešamā informācija (piemēram, QR kods) ir jāsniedz personai, ir otrs faktors⁵⁷ un tādējādi pastiprina autentifikācijas drošību.
42. Attiecībā uz saderību ar VDAR 25. pantu un jo īpaši, lai izpildītu prasību par datu minimizēšanu, jānodrošina, ka apstrāde atbilst nepieciešamības principam. 1. scenārijā izvēlētos pasākumus varētu uzskatīt par tādiem, kas atbilst nepieciešamības principam saistībā ar vēlamo mērķi (proti, racionalizēt pasažieru plūsmu), ja atkarībā no apstrādes apstākļiem pārzinis var pierādīt, ka nav mazāk ierobežojošu alternatīvu risinājumu, ar kuriem tikpat efektīvi varētu sasniegt to pašu mērķi. Piemēram, pārzinis var pierādīt, ka pat tad, kad pasažieriem būtu jāuzrāda sava ierīce, 1. scenārijs paātrinātu pārbaudes procesu salīdzinājumā ar pašreizējo situāciju, kas ietver cilvēka veiktu pārbaudi par to, vai iekāpšanas kartē norādītais vārds un uzvārds atbilst pasažiera personu apliecinošajam dokumentam⁵⁸. To jo īpaši nevarētu pierādīt, ja attiecīgā brīdī netiek veiktas pārbaudes, lai pārbaudītu pasažieru identitāti, pamatojoties uz viņu oficiālo personu apliecinošu dokumentu (šajā saistībā sk. 18. punktu iepriekš tekstā).
43. Turklāt lidostas ekspluatants nesaglabā biometriskās veidnes pēc reģistrācijas, un pārbaudi veicošais pārbaudītājs glabā biometriskos datus ļoti īsu laika periodu, jo šādi dati tiek dzēsti, tiklīdz ir pabeigta atbilstības meklēšana. Tādējādi šķiet, ka 1. scenārijā izvēlētie pasākumi ierobežo personas datu apstrādes apjomu un glabāšanas laiku.
44. Attiecībā uz proporcionalitātes principu šādas apstrādes radītos ierobežojumus var līdzsvarot ar pasažieru aktīvu iesaisti, jo viņu biometriskie dati tiktu glabāti tikai pie pasažieriem. Turklāt, ņemot vērā iepriekš aprakstītos pasākumus un pieņemot, ka pārzinis īsteno atbilstošas garantijas, kas nepieciešamas konkrētajai apstrādei, atbilstošu pasākumu īstenošana varētu nodrošināt riskam atbilstošu drošības līmeni. Šādā gadījumā negatīvo ietekmi uz datu subjektu pamattiesībām un brīvībām varētu uzskatīt par proporcionālu paredzamajam ieguvumam.
45. Tāpēc, ņemot vērā iepriekš minēto, atbildot uz 1.1. jautājumu, kolēģija secina, ka šādu apstrādi **principā varētu uzskatīt par saderīgu ar VDAR 5. panta 1. punkta f) apakšpunktu, 25. un 32. pantu, ja tiek piemērotas atbilstošas garantijas.**

⁵⁵ Pamatnostādnes 05/2022 par sejas atpazīšanu tiesībaizsardzības jomā, 17. punkts.

⁵⁶ Kā aprakstīts turpmāk, sākot no 46. punkta.

⁵⁷ Piemēram, tas mazina izlikšanās risku. Sk. arī garantiju C.1.2. tālāk tekstā.

⁵⁸ Varētu arī apgalvot, ka biometriskās pārbaudes laikā varētu tikt pieļauts mazāk kļūdu nekā cilvēka veiktas pārbaudes gadījumā.

Atbilstošas garantijas

46. Atbildot uz 1.2. jautājumu, šāda veida scenārija gadījumā EDAK uzskata, ka būtu jāīsteno vismaz tālāk tekstā aprakstītās garantijas. Lai sasniegtu tos pašus drošības un datu aizsardzības mērķus, varētu izmantot citas garantijas, kas nav aprakstītas šajā atzinumā, un tās varētu būt likumīgas, ja vien tās nodrošina atbilstību piemērojamajam tiesiskajam regulējumam.
47. Piezīme. Šis ir augsta līmeņa un neizsmeljošs pārskats par iespējamām atbilstošām garantijām, kas pārzinim būtu jāīsteno 1. scenārijam līdzīgā risinājumā. To piemērotība saskaņā ar VDAR 25. un 32. pantu būs atkarīga no katra atsevišķa gadījuma analīzes. Visiem pārziņiem būs jānodrošina, ka tie veic savu novērtējumu par ietekmi uz datu aizsardzību (turpmāk – *DPIA*)⁵⁹, un to konkrētajiem risinājumiem var būt nepieciešami papildu pasākumi, kas nav iekļauti šajā atzinumā.

A. Vispārīgas garantijas

A.1. Novērtējums par ietekmi uz datu aizsardzību

A.1.1. Novērtējumu par ietekmi uz datu aizsardzību saskaņā ar VDAR 35. panta prasībām veic ikreiz, kad pārzinis plāno jaunu apstrādes darbību, kas ietver apstrādi, kura varētu radīt augstu risku. Tā tas varētu būt 1. scenārija gadījumā, jo tas ietver biometrisku datu apstrādi lielā mērogā⁶⁰. Agrīnā izstrādes posmā izvērtē sejas atpazīšanas sistēmas ieviešanas piemērotību, tostarp tās nepieciešamību un proporcionalitāti attiecībā uz sasniedzamajiem mērķiem⁶¹, un to pārskata visā produkta izstrādes dzīves ciklā.

A.1.2. Apspiežas ar attiecīgo uzraudzības iestādi, ja apstrāde joprojām rada augstu risku, neraugoties uz pārziņa veiktajiem riska mazināšanas pasākumiem⁶².

A.2. Datu subjekta tiesības un garantijas, ko var īstenot pārzinī

A.2.1. Garantijas pseidonegatīvu rezultātu novēršanai. Mazina ar vecumu, dzimumu un rasi saistītu noslieču risku, "regulāri novērtē[jot], vai algoritmi darbojas saskaņā ar mērķiem, un pielāgo[jot] algoritmus, lai mazinātu neatklātās noslieces un nodrošinātu apstrādes taisnīgumu"⁶³. Piemēram, īstenojot cilvēka veiktu uzraudzību un iejaukšanos, lai mazinātu jebkādas noslieces un nodrošinātu, ka nenotiek pasažieru stigmatizācija vai profilēšana.

⁵⁹ VDAR 35. pants.

⁶⁰ VDAR 35. panta 3. punkts un 29. panta darba grupas Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (*DPIA*) veikšanai un noteikšanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē, pieņemtas 2017. gada 13. oktobrī, WP248rev.01, apstiprinājusi EDAK.

⁶¹ VDAR 35. panta 7. punkta b) apakšpunkts.

⁶² VDAR 36. panta 1. punkts.

⁶³ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 60. zemsvītras piezīme, 70. punkts.

A.2.2. Nodrošina, ka visa personas datu apstrāde ir pārredzama un ka personas ir informētas un katras apstrādes darbības laikā kontrolē, kā tiek apstrādāti viņu dati⁶⁴.

A.2.3. Nodrošina, ka ir ieviesti pasākumi nolūka ierobežojuma principa ievērošanai, lai dati netiktu izmantoti citiem mērķiem, piemēram, drošības vai apmācības mērķiem.

A.2.4. Nodrošina, ka personām, kuras nepiekrīt sejas atpazīšanai, veicot atbilstošus pasākumus, netiek uzņemtas fotogrāfijas vai video, pat ja tie netiek ierakstīti un apstrādāti (piemēram, izmantojot pietiekamu lauka dziļumu un uztveršanas zonu, lai izvairītos no citu pasažieru attēlu uzņemšanas fonā vai tuvumā, aktivizējot īpašas rindas, kas nepārprotami apzīmētas kā tādas, kas paredzētas sejas atpazīšanai).

A.2.5. Ja tās pašas iekārtas var izmantot pasažieri, kas piekrīt sejas atpazīšanai, un pasažieri, kas tai nepiekrīt, vai ja pasažieri, kas nepiekrīt sejas atpazīšanai, var parādīties redzes laukā, kamēr sistēma netiek izmantota, pirms fotografēšanas vai video ierakstīšanas sākuma gaida aktīvu tāda pasažiera darbību, kas devis piekrišanu.

A.2.6. Iespēja datu subjektam jebkurā laikā dzēst datus, kas atrodas tikai pie viņa (biometriskā veidne⁶⁵) mobilajā lietotnē vai digitālajā makā⁶⁶.

A.2.7. Pastāv dzīvotspējīgas alternatīvas vai rezerves risinājumi (t. i., pasažieriem, kuri nepiekrīst savu biometrisko datu izmantošanai, pasažieriem, kuri nevarētu izmantot šādus risinājumus, vai pasažieriem, kurus kļūdaini noraidītu), lai cita starpā nodrošinātu, ka pasažieriem, kuri nav devuši savu piekrišanu, nerastos nekāds kaitējums⁶⁷.

A.2.8. Ja izmanto lietotni, tā būtu rūpīgi jāizstrādā un jākonfigurē tā, lai nevāktu nevajadzīgus datus un lai izvairītos no jebkādu tādu trešo personu programmatūras izstrādes komplektu (PIK) izmantošanas, kas vāc datus citiem nolūkiem.

A.3. Pārskatatbildība

A.3.1. Novērtē, vai pastāv kādi attiecīgi rīcības kodeksi vai sertifikācijas mehānismi, lai palīdzētu pierādīt atbilstību apstrādes drošības prasībām, kas noteiktas VDAR 32. pantā⁶⁸. Pārbauda, vai pasākumi ir piemēroti konkrētajai apstrādei. Standarti⁶⁹, paraugprakse un

⁶⁴ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 68. punkts, un VDAR 7. apsvērumš.

⁶⁵ Atsauces uz biometrisko veidni 1. scenārija garantijās atbilst atsaucēm uz atslēgu / slepeno paroli 2. scenārijā.

⁶⁶ Ņemiet vērā, ka šī garantija attiecas tikai uz 1. scenāriju.

⁶⁷ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 86. punkts.

⁶⁸ VDAR 32. panta 3. punkts un EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 10. punkts.

⁶⁹ Sk., piemēram, ISO/IEC 2382–37.

rīcības kodeksi, ko atzinušas asociācijas un citas struktūras, kas pārstāv pārziņu kategorijas, var palīdzēt noteikt piemērotus pasākumus.

A.3.2. Nodrošina, ka lietotāja ierīcei tiek veiktas pamata drošības pārbaudes, lai būtu iespējama reģistrācija, tomēr pasažierim ir arī noteikta loma savu datu aizsardzībā, jo tie tiek glabāti viņa ierīcē. Šādu tehnisko pārbaūžu un kontroļu piemēri ir sniegti C.2. iedaļā "Infrastruktūra un tīkls".

B. Organizatoriskas garantijas

B.1. Politika un atbilstība

B.1.1. Nodrošina, ka ir ieviesta iekšējā piekļuves kontrole⁷⁰ ar noteikumiem administratoriem.

B.1.2. Ja sejas atpazīšanas pakalpojumu var sniegt viena no personām, kas iesaistīta apstrādē bez identifikācijas vai biometriskajiem, vai abu veidu datiem, kuri ir jāapstrādā citām iesaistītajām personām, aizliedz šo datu plūsmu caur minētajām citām personām. Piemēram, aviosabiedrībai nav tehniski jāpiekļūst biometriskajiem datiem, ja tā izmanto lidostas kopējo infrastruktūru, pat ja šī aviosabiedrība darbojas kā datu apstrādes pārzinis saskaņā ar VDAR.

B.1.3. Definē šifrēšanas un atslēgu pārvaldības politiku⁷¹, piemēram, attiecībā uz identifikācijas un biometrisko datu apstrādi.

B.1.4. Nodrošina atbilstību VDAR V nodaļai. Piemēram, lai nodrošinātu atbilstīgu nosūtīšanu, ja pārzinis reģistrācijas procesā izmanto attālinātu pakalpojumu, kas atrodas trešā valstī.

B.1.5. Ja izmanto apstrādātājus, nodrošina, ka ar to ir noslēgta vienošanās⁷² saskaņā ar VDAR 28. panta 3. punktu.

B.1.6. Nodrošina, ka ir ieviestas procedūras, lai pārvaldītu cilvēka veiktu uzraudzību un iejaukšanos, jo īpaši, lai risinātu nepatīkamas noraidīšanas problēmas un tehniskas vai lietojamības problēmas.

B.2. Apmācība un testēšana

B.2.1. Nodrošina, ka personāls ir pienācīgi apmācīts.

⁷⁰ EDAK Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu, pieņemtas 2020. gada 21. aprīlī (turpmāk – **EDAK Pamatnostādnes 4/2020 par atrašanās vietas datu un kontaktu izsekošanas rīkiem**), SEC-10, 16. lpp.

⁷¹ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 89. punkts.

⁷² VDAR 28. panta 3. punkts.

B.2.2. Īsteno "procesu regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību"⁷³.

B.2.3. Īsteno procesu, lai nodrošinātu, ka pasažiera biometriskās veidnes apstrāde⁷⁴ autentifikācijas nolūkos ir tehniski efektīva un pietiekami precīza.

B.2.4. Nodrošina, ka biometriskie paraugi, kas savākti gan reģistrācijas laikā, gan kontrolpunktā, ir pietiekami kvalitatīvi, lai veiktu uzticamu biometrisku apstrādi.

C. Tehniskas garantijas

C.1. Piekļuve

C.1.1. Reģistrācijas posmā īsteno garantijas, lai pilnībā nodrošinātu reģistrācijas procesu ar pārbaudītu identitāti. Piemēram, lai pastiprinātu lietotāju identitātes novērtēšanu ar vairākfaktoru autentifikāciju, var veikt pasākumus, sākot no vienreizējām ar paroli aizsargātām saitēm un beidzot ar lietotnes aktivizēšanu un vietējas ierīces atbloķēšanas mehānismiem.

C.1.2. Īsteno garantijas, lai novērstu pseidopozitīvus rezultātus, krāpnieciskas identitātes izveides uzbrukumus un krāpšanu⁷⁵.

C.1.3. Aizliedz jebkādu ārēju piekļuvi identifikācijas un biometriskajiem datiem⁷⁶.

C.1.4. Nodrošina, ka apstrādi veic uz vietas reģistrācijas, nosūtīšanas un atbilstības meklēšanas posmos. Atbilstības meklēšanas punktam jābūt pēc iespējas tuvāk personas ierīcei. Lai nodrošinātu veidnes atbilstības atsevišķai ierīcei pārbaudi, varētu būt nepieciešama mijiedarbība ar ārpus lidostas esošiem pakalpojumu sniedzējiem, kas ietver publisko tīklu resursu izmantošanu un kas varētu negatīvi ietekmēt pieejamību un veidnes izplatīšanu ārējām struktūrām.

C.1.5. Autenticē lietotāju, lai pievienotu jaunu lidojumu un ģenerētu jaunu šifrētu QR kodu.

C.1.6. Īsteno pasākumus, lai risinātu situāciju, kad pasažieris var zaudēt piekļuvi savam QR kodam.

C.2. Infrastruktūra un tīkls

⁷³ VDAR 32. panta 1. punkta d) apakšpunkts.

⁷⁴ Atsauces uz biometrisku veidni 1. scenārija garantijās atbilst atsaucēm uz atslēgu / slepeno paroli 2. scenārijā.

⁷⁵ ENISA 2022. gada janvāra Ziņojums par digitālo identitāti – par decentralizēti pārvaldītas identitātes (*Self-Sovereign Identity, SSI*) koncepcijas izmantošanu, lai veidotu uzticēšanos.

⁷⁶ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 89. punkts.

C.2.1. Nosacījumus par operētājsistēmu (OS) pastāvīgi atjaunina un nodrošina autentifikāciju, lai varētu piekļūt ierīcei lietojumprogrammas / digitālā maka darbības nolūkā, cita starpā automātiski izdzēšot identifikācijas un biometriskos datus, ja operētājsistēma ir novecojusi un rada drošības riskus.

C.2.2. Atbilstības meklēšanas iekārtu izolē no tīkla ekspluatācijas laikā un veic visus pārējos drošības garantēšanai nepieciešamos pasākumus.

C.2.3. Veic biometrisko datu atbilstības meklēšanu pasažiera ierīcē vai iekārtā (*edge computing*).

C.2.4. Risinājumi pasažieru individuālo ierīču drošības vājo vietu novēršanai, cita starpā veicot (vismaz) biometrisko un identifikācijas datu šifrēšanu laikā, kad ierīce netiek lietota.

C.2.5. Izmanto (vismaz) biometrisko datu drošu glabāšanu tikai pie lietotāja⁷⁷, piemēram, drošā viedtālruņa sadaļā.

C.2.6. Drošības garantijas, lai nodrošinātu telpu, arī lidostas biometriskā termināļa, fizisko drošību. Nodrošina augstu to arhitektūras elementu drošības līmeni, kas apstrādā identifikācijas un biometriskos datus (piemēram, datošana, datu plūsma, īslaicīga vai ilgtermiņa glabāšana).

C.3. Lietotāja identitātes pārbaudes datu drošība un pārvaldība

C.3.1. Nosūtīšanas un glabāšanas laikā datus sadala vismaz trīs dažādās grupās, piemēram, identifikācijas dati, biometriskie dati un lidojuma dati⁷⁸. Nodrošina, ka dati laikā starp nosūtīšanu un glabāšanu tiek pienācīgi šifrēti.

C.3.2. Ievieš tehniskus pasākumus, lai nodrošinātu, ka attiecīgajā kontrolpunktā tiek apstrādāti un pārbaudīti tikai tie dati, kurus var likumīgi apstrādāt konkrētos kontrolpunktos.

C.3.3. Nodrošina datu dzēšanas efektivitāti⁷⁹, izmantojot drošu dzēšanas procedūru (piemēram, galveno atmiņu, kešatmiņu, iespējamās dublējumkopijas), un novērtē, kad datu dzēšanai vajadzētu būt automatizētai. Datu glabāšanas termiņi būtu stingri jāievēro, izmantojot automātisku kārtību, un personai nav jāveic papildu darbības⁸⁰.

⁷⁷ Atsauces uz biometrisko veidni 1. scenārija garantijās atbilst atsaucēm uz atslēgu / slepeno paroli 2. scenārijā.

⁷⁸ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 89. punkts.

⁷⁹ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 89. punkts.

⁸⁰ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integritātes datu aizsardzība un datu aizsardzība pēc noklusējuma, 82. punkts.

C.3.4. Nodrošināt datu autentiskumu un integritāti (piemēram, paraksts)⁸¹.

C.3.5. Pasažieru biometriskos datus reģistrācijas punktā un kontrolpunktā saglabā tikai ļoti īsu laiku un tos dzēš, tiklīdz pasažieris ir šķērsojis kontrolpunktu.

C.3.6. Ja reģistrācijai izmanto lietotni, lietojumprogrammas izstrādes laikā piemēro mobilo lietojumprogrammu drošības standartus, kā arī izmanto trešo personu veiktus drošības testus.

C.3.7. Reģistrācijas posmā lidostā nodrošina drošības pasākumus, lai saglabātu pasažieru biometrisko datu konfidencialitāti un integritāti. Piemēram, ja QR kodu izdrukā kioskā, to kioskā nevajadzētu rādīt, lai novērstu iespēju, ka ļaunprātīgs dalībnieks uzņem attēlu. Ja pārraide notiek nelielā attālumā, tā būtu jāveic, pamatojoties uz lietotāja aktīvu iesaistīšanos un izmantojot kanālu, kas nodrošina nelielu attālumu.

C.3.8. Dati, kas ir vienīgi personas rīcībā⁸², būtu droši jāglabā personas ierīcē, un visām iespējamām ievainojamībām, kas saistītas ar ierīces operētājsistēmām, ir jāpiemēro atbilstoši drošības ielāpi. Drukāta QR koda gadījumā persona būtu jāinformē par tajā ietverto datu īpaši sensitīvo raksturu un koda piedāvātajām iespējām.

C.3.9. Nodrošina reģistrāciju, izmantojot identitātes attālinātas pārbaudes atbilstošas metodes⁸³.

3.2.2 2. scenārijs – reģistrētās biometriskās veidnes centralizēta glabāšana šifrētā veidā lidostā, atslēgai / slepenajai parolei atrodoties tikai pie pasažiera, lai veiktu autentifikāciju

48. Šajā iedaļā aplūkota autentifikācijas nolūkos veiktas pasažieru reģistrēto biometrisko veidņu centralizētas glabāšanas, kas notiek šifrētā veidā un atslēgai / slepenajai parolei atrodoties tikai pie pasažiera, saderība ar VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu⁸⁴ (turpmāk – **2. scenārijs**). Šajā iedaļā ir arī aplūkotas 2. scenārijam atbilstošas garantijas, ņemot vērā VDAR 25. un 32. pantu.

Scenārija apraksts

49. 2. scenārijā reģistrācija tiek veikta tikai vienu reizi un uz noteiktu derīguma periodu (piemēram, vienu gadu pēc pēdējā lidojuma, līdz pases derīguma termiņa beigām) – vai nu attālināti ar atbilstošu identitātes garantijas līmeni (piemēram, eIDAS atbilstošu pārliecības līmeni), vai arī lidostas termināļos. Reģistrāciju kontrolē lidostas ekspluatants, un tā ietver tādu identifikācijas un biometrisko datu ģenerēšanu, kas šifrēti ar atslēgu / slepenu paroli.

⁸¹ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 89. punkts.

⁸² Atsauces uz biometrisko veidni 1. scenārija garantijās atbilst atsaucēm uz atslēgu / slepenu paroli 2. scenārijā.

⁸³ Sk. ENISA, Ziņojums par attālinātu identifikācijas pārbaudi. Analīze par metodēm identitātes pārbaudes attālinātai veikšanai, 2021. gada marts.

⁸⁴ Kā piemēru var minēt 2. lietošanas gadījumu, kas aprakstīts pieprasījuma I pielikumā.

50. Datubāze tiek glabāta lidostas telpās lidostas ekspluatanta kontrolē. Individuālas šifrēšanas atslēgas / slepenās paroles tiek glabātas tikai personas ierīcē (piemēram, lidostas ekspluatanta mobilajā lietotnē). Lietotne var ģenerēt QR kodu, kas satur atslēgu / slepenu paroli, ko var izdrukāt uz papīra vai parādīt ierīces ekrānā⁸⁵. Turklāt lidostas ekspluatants īsteno otro šifrēšanas slāni⁸⁶, kura atslēgas kontrolē lidostas ekspluatants.
51. Pasažieri tiek autentificēti (tieša salīdzināšana), kad viņus pārbauda īpašos kontrolpunktos lidostā. Pasažieri, kuri izvēlas izmantot biometriskos kontrolpunktus, parāda savu QR kodu īpašai kontroles iekārtai, kas aprīkota ar QR skeneri un kameru. Pasažieru indekss tiek nosūtīts uz datubāzi, lai pieprasītu šifrēto veidni, ko lejupielādē un pārbauda uz vietas iekārtā un/vai lietotāja ierīcē. Kontrolpunktā esošajam pārbaudītājam ir zināms tikai atbilstošais rezultāts, ko tas izmanto⁸⁷.
52. Šajā scenārijā nav identifikācijas un biometrisko datu plūsmu starp lidostām, un starp centralizētajām datubāzēm nav ne starpsavienojumu, ne sadarbības.

EDAK novērtējums

53. 2. scenārijā pasažieru reģistrētās biometriskās veidnes tiek glabātas centralizēti, bet šifrētā veidā un ar atslēgu / slepenu paroli, kas atrodas tikai pie pasažieriem. 2. scenārijā pasažieri tiek autentificēti (tieša salīdzināšana).
54. Šajā scenārijā tiek ierosināts, ka mērķi racionalizēt pasažieru plūsmu (t. i., palielinot pārbaudes ātrumu) varētu sasniegt, izmantojot centralizētu sistēmu. EDAK iepriekš ir norādījusi, ka šādu risinājumu varētu uzskatīt par dzīvotspējīgu alternatīvu reģistrētu biometrisko veidņu decentralizētai glabāšanai⁸⁸ (kā aprakstīts 1. scenārijā), ja ir objektīvas vajadzības un tiek izmantotas atbilstošas garantijas (sk. 60. punktā aprakstītās garantijas).
55. Attiecībā uz drošības apsvērumiem jānorāda, ka katras personas dati tiek šifrēti ar konkrētu atslēgu, ko glabā tikai šī persona un kas ir tikai šīs personas kontrolē. Turklāt tas, ka atbilstības meklēšanai nepieciešamā informācija (proti, slepenā parole / atslēga) ir jāsniedz personai, ir otrs faktors⁸⁹ un tādējādi pastiprina autentifikācijas drošību. Turklāt lidostas ekspluatants īsteno otro šifrēšanas slāni, kura atslēgas kontrolē lidostas ekspluatants. 2. scenārijā personas indekss tiek nosūtīts uz centrālo datubāzi, lai izgūtu ar personu saistītos biometriskos datus. Pēc tam šos datus nosūta (šifrētā veidā) uz datoru, kas atrodas kontrolpunktā, kur tos atšifrē, lai veiktu atbilstības meklēšanu, un kontrolpunktā esošajam pārbaudītājam ir zināms tikai atbilstības meklēšanas rezultāts, ko tas izmanto. Ja personas atslēga / slepenā parole tiek saglabāta kontrolpunktā izvietotajā datorā un uz centrālo

⁸⁵ FR UI ir sīkāk precizējusi, ka pieprasītās informācijas nosūtīšanai varētu būt arī citi tehniski risinājumi, piemēram, izmantojot tuvas darbības sakaru protokolu.

⁸⁶ Atslēga / slepenā parole (atrodas pie personas) pati ir šifrēta ar citu atslēgu, kas atrodas pie lidostas ekspluatanta.

⁸⁷ FR UI paskaidroja, ka šis glabāšanas periods ir ilustratīvs un ka to var uzskatīt par pieņemamu, ņemot vērā, ka atslēga atrodas pie personām un to var izvēlēties reģistrācijas posmā. Tomēr jānorāda, ka šādu glabāšanas laiku var pielāgot.

⁸⁸ EDAK Pamatnostādnes 3/2019 par videoierīcēm, 88. punkts.

⁸⁹ Piemēram, tas mazina izlikšanās risku. Sk. arī garantiju C.1.2. tālāk tekstā.

datubāzi tiek nosūtīts tikai pasažiera indekss, lai atgūtu šifrēto biometrisko veidni, šādus drošības pasākumus varētu uzskatīt par saderīgiem ar VDAR 5. panta 1. punkta f) apakšpunktu un 32. pantu.

56. Attiecībā uz saderību ar VDAR 25. pantu un jo īpaši, lai izpildītu prasību par datu minimizēšanu, jānodrošina, ka apstrāde atbilst nepieciešamības principam. 2. scenārijā izvēlētos pasākumus varētu uzskatīt par tādiem, kas atbilst nepieciešamības principam saistībā ar vēlamo mērķi (proti, racionalizēt pasažieru plūsmu lidostās), ja atkarībā no apstrādes apstākļiem pārzinis var pierādīt, ka nav mazāk ierobežojošu alternatīvu risinājumu, ar kuriem tikpat efektīvi varētu sasniegt to pašu mērķi. 2. scenārijā pasažieriem joprojām būtu jāuzrāda sava ierīce⁹⁰. Tomēr pārzinis var pierādīt, ka 2. scenārijs paātrina pārbaudes procesu salīdzinājumā ar pašreizējo situāciju, kas ietver cilvēka veiktu pārbaudi par to, vai iekāpšanas kartē norādītais vārds un uzvārds atbilst pasažiera personu apliecinošajam dokumentam⁹¹, vai salīdzinājumā ar 1. scenāriju. To jo īpaši nevarētu pierādīt, ja attiecīgā brīdī netiek veiktas pārbaudes, lai pārbaudītu pasažieru identitāti, pamatojoties uz viņu oficiālo personu apliecinošu dokumentu (šajā saistībā sk. 18. punktu iepriekš tekstā).
57. Attiecībā uz proporcionalitātes principu šādas apstrādes radītos ierobežojumus var līdzsvarot ar to pasažieru aktīvu iesaisti, kuri vienīgie kontrolē savu šifrēto datu atslēgu. Turklāt ņemiet vērā, ka drošības riskus, ko rada pasažieru biometrisko datu glabāšana centralizētā datubāzē, kad atslēga atrodas tikai pie pasažieriem, var mazināt, izmantojot atbilstošas garantijas (sk. garantijas, kas norādītas 60. punktā tālāk tekstā). Tāpēc pieņemot, ka pārzinis īsteno atbilstošas garantijas, kas nepieciešamas attiecīgajai konkrētajai apstrādei, drošības risku personām varētu mazināt un negatīvo ietekmi uz datu subjektu pamattiesībām un brīvībām varētu uzskatīt par proporcionālu paredzamajam ieguvumam. Protams, visos gadījumos būtu jānodrošina, ka tiek apstrādāti tikai šim nolūkam vajadzīgie dati un ka tiek pārbaudīti tikai tie pasažieri, kas tam piekrituši; tādējādi nepastāv risks, ka tiks vākti citu pasažieru, kuri nav devuši piekrišanu, biometriskie dati.
58. Pieprasījumā kā piemērs ir minēts, ka 2. scenārijā šifrēto datu glabāšanas termiņš datubāzē parasti varētu būt viens gads pēc pēdējā lidojuma, ko veikusi persona, un līdz pases derīguma termiņa beigām. Pieprasījumā nav sniegta informācija, lai ar objektīviem iemesliem pamatotu tik ilgu laika posmu, tomēr var pieņemt, ka šāds glabāšanas periods ir paredzēts turpmāku lidojumu ērtas veikšanas labad. Attiecībā uz glabāšanas periodu jānorāda, ka, lai šā scenārija gadījumā panāktu saderību ar VDAR 5. panta 1. punkta e) apakšpunktu, pārziniem būtu jāspēj pamatot, kāpēc paredzētais glabāšanas periods konkrētos gadījumos ir nepieciešams, lai īstenotu šo nolūku. Kolēģija iesaka pārziniem paredzēt pēc iespējas īsāku glabāšanas laiku, ņemot vērā arī pasažierus, kuri veic lidojumus ļoti reti, un piedāvāt datu subjektiem noteikt vēlamo glabāšanas laiku.
59. Ņemot vērā šos apsvērumus, atbildot uz 2.1.1. jautājumu, kolēģija secina, ka šādu apstrādi **principā varētu uzskatīt par saderīgu ar VDAR 5. panta 1. punkta e) un f) apakšpunktu, 25. un 32. pantu, ja tiek piemērotas atbilstošas garantijas.**

⁹⁰ FR UI ir sīkāk precizējusi, ka varētu būt arī citas iespējas iesniegt veidni, piemēram, uz papīra izdrukātā veidā. Turklāt EDAK atzīst, ka nākotnē varētu paredzēt izmantot alternatīvu tehnoloģiju, piemēram, pamatojoties uz tuvā lauka sakaru sistēmu.

⁹¹ Varētu arī apgalvot, ka biometriskās pārbaudes laikā varētu tikt pieļauts mazāk kļūdu nekā cilvēka veiktas pārbaudes gadījumā.

Atbilstošas garantijas

60. Atbildot uz 2.1.2. jautājumu, šāda veida scenārija gadījumā kolēģija uzskata, ka **papildus 1. scenārijā uzskaitītajām garantijām** būtu jāīsteno vismaz tālāk tekstā aprakstītās garantijas. Lai sasniegtu tos pašus drošības un datu aizsardzības mērķus, varētu izmantot citas garantijas, kas nav aprakstītas šajā atzinumā, un tās varētu būt likumīgas, ja vien tās nodrošina atbilstību piemērojamajam tiesiskajam regulējumam.
61. Piezīme. *Šis ir augsta līmeņa un neizsmeļošs pārskats par iespējamām atbilstošām garantijām, kas pārzinim būtu jāīsteno 2. scenārijam līdzīgā risinājumā. To piemērotība saskaņā ar VDAR 25. un 32. pantu būs atkarīga no katra atsevišķa gadījuma analīzes. Visiem pārziņiem būs jānodrošina, ka tie veic savu DPIA, un to konkrētajiem risinājumiem var būt nepieciešami papildu pasākumi, kas nav iekļauti šajā atzinumā.*

D. Vispārīgas garantijas

D.1. Datu subjekta tiesības un garantijas, ko var īstenot pārziņi

D.1.1. Nodrošina, ka pasažieris kontrolē visu savu datu glabāšanas periodus. Glabāšanas laiks nedrīkstētu būt garāks par to, kas nepieciešams konkrētajam nolūkam. Pēc rūpīgas tādu faktoru analīzes kā identifikācijas dokumenta derīgums būtu jānosaka maksimālais termiņš. Datu subjektiem būtu jāpiedāvā noteikt vēlamo glabāšanas laiku, kas varētu būt īsāks par noklusējuma glabāšanas periodu.

D.1.2. Iespēja datu subjektam jebkurā laikā pieprasīt dzēst datus, kas atrodas tikai pie viņa (atslēga / slepenā parole) mobilajā lietotnē vai digitālajā makā⁹².

D.1.3. Centrālās datubāzes atrašanās vieta ļauj kompetentajai uzraudzības iestādei veikt efektīvu uzraudzību.

E. Organizatoriskas garantijas

E.1. Politika un atbilstība

E.1.1. Uzticībai centrālajam serverim jābūt ierobežotai. Centrālā servera pārvaldībā jāievēro skaidri definēti pārvaldības noteikumi un jāīsteno visi pasākumi, kas vajadzīgi, lai garantētu tā drošību⁹³.

F. Tehniskas garantijas

⁹² Nemiet vērā, ka šī garantija attiecas tikai uz 2. scenāriju.

⁹³ EDAK Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu, PRIV-5, 17. lpp.

F.1. Piekļuve

F.1.1. Uztur reģistrus par to, kam ir piekļuve personas datiem, jo īpaši identifikācijas un biometriskajiem datiem, un par piekļuves šiem datiem laiku.

F.2. Infrastruktūra un tīkls

F.2.1. Atbilstoši aizsargā centrālo datubāzi, tostarp pret uzbrukumiem, kas saistīti ar pieejamību.

F.2.2. Nodrošina, ka nav interneta pieslēguma centrālajai datubāzei, reģistrācijas iekārtām un atbilstības meklēšanas blokiem. Šīs sistēmas ekspluatācija un uzturēšana (piemēram, dublēšana, ielāpu piemērošana, uzraudzība utt.) jāveic uz vietas lidostas telpās.

F.3. Datu drošība un pārvaldība

F.3.1. Ievieš mūsdienīgas kriptogrāfijas tehnikas, lai garantētu drošu apmaiņu starp lietotni un centralizēto serveri⁹⁴.

F.3.2. Atsevišķo atslēgu / slepeno paroli glabā līmenī, kurā tā tiks izmantota atšifrēšanai (t. i., iekārtā), un indeksu izmanto, tikai lai centrālajā datubāzē atgūtu attiecīgo reģistrēto biometrisko veidni.

F.3.3. Nodrošina, ka atslēgas / slepenās paroles apmaiņa starp lietotāja ierīci un iekārtu aizsargā saziņu no jebkādas iespējamās noklausīšanās vai nosūtīšanas trešām personām.

F.3.4. Biometrisko veidni indeksē, kad tā tiek glabāta centrālajā datubāzē, lai dotu iespēju veikt autentifikāciju 1:1 un nodrošinātu, ka tā ir unikāla un saistīta ar attiecīgo personu. Nodrošina, ka indekss neatklāj nekādu pasažiera identifikācijas informāciju un nav saistīts ar šifrēšanas atslēgu.

F.3.5. Atbilstoši autentificē un šifrē jebkādu nosūtīšanu no centrālās datubāzes uz kontrolpunktiem un otrādi, un to veic izolētos tīklos.

F.3.6. Izvairās no divvirzienu saites starp datu kopām (identifikācijas dati un biometriskie dati, kā arī informācija par lidojumu) un datubāzē saglabā tikai attiecīgas vienvirziena

⁹⁴ EDAK Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu, SEC-4, 16. lpp. "Tehniskie paņēmieni, ko var izmantot, ir, piemēram, šādi: simetriska un asimetriska šifrēšana, jaucējfunkcijas, privātas piederības tests, privātas kopas krustpunkts, Blūma filtri, privātas informācijas izguve, homomorfa šifrēšana utt."

saites. Piemēram, tikai vienvirziena saites no indeksa uz identifikācijas datiem, no indeksa uz šifrētiem biometriskajiem datiem un no indeksa uz informāciju par lidojumu.

F.3.7. Īsteno darbības nepārtrauktības nodrošināšanas pasākumus, piemēram, ieviešot atbilstošas dublējumkopiju uzglabāšanas sistēmas.

F.3.8. Nodrošina, ka iekārta neuztur šifrētu vai nešifrētu veidņu žurnālus.

3.2.3 Reģistrēto biometrisko veidņu centralizēta glabāšana, lai veiktu identifikāciju

62. Šajā iedaļā aplūkota autentifikācijas nolūkos veiktas pasažieru reģistrēto biometrisko veidņu centralizētas glabāšanas saderība ar VDAR 5. panta 1. punkta e) un f) apakšpunktu un 25. un 32. pantu, ja šādas veidnes nav šifrētas ar atslēgu / slepenu paroli, kas atrodas tikai pie pasažiera, divos lietošanas gadījumos: 1) ja šādas veidnes tiek glabātas lidostā esošā datubāzē, ko kontrolē lidostas ekspluatants⁹⁵ (turpmāk – **3.1. scenārijs**), un 2) ja šādas veidnes tiek glabātas mākonī, ko kontrolē aviosabiedrība⁹⁶ (turpmāk – **3.2. scenārijs**).
63. Kolēģija uzskata, ka biometrisko datu izmantošana **identifikācijas** nolūkos lielās centrālajās datubāzēs ir pretrunā datu subjektu pamattiesībām un varētu radīt nopietnas sekas datu subjektiem⁹⁷. Turklāt biometrisko datu izmantošana būtu jāizskata arī saistībā ar to apstrādes nolūku, ņemot vērā nepieciešamības un proporcionalitātes principus⁹⁸.

3.2.3.1 3.1. scenārijs – centralizēta glabāšana lidostā esošā datubāzē lidostas ekspluatanta kontrolē

Scenārija apraksts

64. 3.1. scenārijā pasažieru reģistrētā biometriskā veidne tiek glabāta centrālā datubāzē lidostas telpās un lidostas ekspluatanta kontrolē šifrētā veidā. Konkrētāk, pasažieru dati ir sadalīti daļās, kas nozīmē, ka viņu identifikācijas dati, reģistrētā biometriskā veidne un informācija par lidojumu tiek glabāta trīs dažādās datubāzēs. Šādi dati tiek šifrēti ar dažādām atslēgām gan glabāšanas laikā, gan laikā, kad tos nosūta uz serveriem, kas veic salīdzināšanu, kur tos pēc tam atšifrē lidostas ekspluatants.
65. Pasažieriem ir jāreģistrējas katram lidojumam īsi pirms izlidošanas (piemēram, 48 stundu laikā). Šādu reģistrāciju var veikt attālināti vai lidostas termināļos ar atbilstošu identitātes garantijas līmeni (piemēram, *eIDAS* atbilstošu pārlicības līmeni). Vai arī reģistrācija var notikt tādā pašā veidā, kā aprakstīts 1. scenārijā, un šajā gadījumā pasažieriem 48 stundu laikā pirms izlidošanas savi dati ir jānosūta no saviem digitālajiem makiem uz lidostas sistēmu.

⁹⁵ Kā piemēru var minēt 3.A lietošanas gadījumu, kas aprakstīts pieprasījuma I pielikumā.

⁹⁶ Kā piemēru var minēt 3.B lietošanas gadījumu, kas aprakstīts pieprasījuma I pielikumā.

⁹⁷ Piemēram, sk. 29. panta darba grupas Atzinumu 3/2012 par biometrijas tehnoloģiju attīstību, 8. lpp. Sk. arī 26. punktu iepriekš tekstā.

⁹⁸ VDAR 4. apsvērumš. Sk. arī 29. panta darba grupas Atzinumu 3/2012 par biometrijas tehnoloģiju attīstību, 8. lpp.

66. Arī šajā gadījumā pasažieri dodas uz īpašu kontroles iekārtu, kas aprīkota ar kameru. Pēc tam pasažieru biometriskais paraugs tiek nosūtīts uz lidostas centrālo serveri, kas mēģinās salīdzināt šos datus ar centrālās biometrisko datu bāzes datiem. Tādējādi var identificēt pasažieri, kā arī pārbaudīt, vai viņš patiešām ir reģistrēts izlidojošajam lidojumam (vai lidojumam, kurā notiek iekāpšana, ja kontrole tiek veikta iekāpšanas brīdī). Atkarībā no kontrolpunkta to datu apjomu, kas nosūtīti atpakaļ kontrolpunktā esošajam pārbaudītājam, kas veicis pieprasījumu, var samazināt līdz minimumam, piemēram, sūtot "jā/nē atbildi" vai pašu atbilstošo rezultātu, ja tas ir vajadzīgs. Šajā gadījumā kontrolpunktā esošajam pārbaudītājam tiek nosūtīts tikai pieprasījuma rezultāts, ko tas izmanto.
67. Konkrētāk, šajā scenārijā tiek identificēti pasažieri (salīdzinājums 1:N), kur N ir paredzamais pasažieru skaits lidostā vairāku dienu laikā. Turklāt biometrisko datu salīdzināšana tiek veikta tikai tad, kad ikviens pasažieris ierodas iepriekš noteiktos izlidošanas lidostas kontrolpunktos, bet pati datu apstrāde notiek centrālā serverī, kas savienots ar centrālo datubāzi. Šajā scenārijā paredzētais glabāšanas laiks parasti ir 48 stundas, un dati tiek dzēsti, tiklīdz lidmašīna ir pacēlusies.

EDAK novērtējums

68. Kā atgādināts iepriekš, biometrisko datu apstrāde ir saistīta ar lielāku risku datu subjektu tiesībām un brīvībām⁹⁹. Tādējādi jebkura datu drošības problēma var radīt īpaši smagas sekas datu subjektiem¹⁰⁰. Pārziņiem ir pienākums efektīvi mazināt šo risku. Tā kā šajā scenārijā visa arhitektūra ir pilnībā centralizēta, pasažieri kontroli pār saviem datiem zaudē lielākā mērā. Turklāt ir arī lielāks risks, ka dati tiks apstrādāti citiem mērķiem, kas atšķiras no pasažieru plūsmas kontroles.
69. Ņemot vērā drošības principu un prasības (VDAR 5. panta 1. punkta f) apakšpunkts un 32. pants), būtu jāuzskata, ka identifikācijas un biometrisko datu glabāšana centrālās datubāzēs, kas, lai gan atsevišķas, var kļūt par īpaši vērtīgu uzbrukuma mērķi, un šādas datubāzes konfidencialitātes pārkāpums var nozīmēt piekļuvi visam datu kopumam. Līdz ar to iespējamais pārkāpums attiecībā uz sejas atpazīšanas veidnēm un ar tām saistīto identitāti var dot iespēju neatļauti vai nelikumīgi identificēt datu subjektus citās situācijās. Atkarībā no biometriskajai identifikācijai izmantotajām metodēm tas var arī apdraudēt sejas atpazīšanas veidņu turpmāku drošu izmantošanu identifikācijas nolūkos. Atšķirībā no cita veida apliecinājumiem (piemēram, lietotāja ID, parole), ko ir iespējams mainīt, šādā gadījumā pārkāpuma sekas nevar mazināt¹⁰¹.
70. Turklāt identifikācijas datu un biometrisko datu, kas ir pārziņa rīcībā, lielais daudzums un augstā kvalitāte padara tos par ļoti vērtīgu uzbrucēja mērķi, kas drošības riska ziņā nozīmē augstāku iespējamību. Turklāt datu aizsardzības pārkāpumiem varētu būt lielāka ietekme, jo, glabājot datus centralizētā vietā, uzbrucējiem varētu būt vieglāk piekļūt personas datiem, kas attiecas uz vairākiem pasažieriem. Tāpēc iespējams pārkāpums lielam datu subjektu skaitam varētu radīt augstu risku saistībā ar pārkāpuma smaguma pakāpi, piemēram, plaša mēroga identitātes zādzība, ko ir ārkārtīgi grūti mazināt.

⁹⁹ Skatīt 26. punktu iepriekš tekstā.

¹⁰⁰ Pamatnostādnes par sejas atpazīšanu, Eiropas Padomes Konvencijas par indivīda aizsardzību attiecībā uz personas datu automatisko apstrādi konsultatīvā komiteja, 2021. gada jūnijs, 22. lpp.

¹⁰¹ Par šo skatīt 29. panta darba grupas Atzinumu 3/2012 par biometrijas tehnoloģiju attīstību, 34. lpp.

71. Tāpēc attiecībā uz saderību ar VDAR 5. panta 1. punkta f) apakšpunktu un 32. pantu 3.1. scenārijā¹⁰² paredzētie pasākumi, ņemot vērā jaunākos sasniegumus, nav pietiekami, lai nodrošinātu riskam atbilstošu drošības līmeni. Pamatojoties uz minēto, 3.1. scenārijā paredzētā apstrāde neatbilstu VDAR 5. panta 1. punkta f) apakšpunktam un 32. pantam, ja pārzinis izmantotu tikai šos pasākumus.
72. Ņemot vērā VDAR 5. panta 1. punkta e) apakšpunktā noteikto principu, šajā scenārijā paredzētais biometrisko datu glabāšanas centrālajā datubāzē periods parasti ir 48 stundas. Šķiet, ka šāds glabāšanas ierobežojums ievērojami samazina risku, kas saistīts ar personas datu aizsardzības pārkāpumiem. Tomēr datu glabāšanas periods pats par sevi nav izšķirošs faktors, lai noteiktu minētās arhitektūras vispārējo saderību, jo datu pārziņi šādus glabāšanas periodus var mainīt. Jebkurā gadījumā ierosinātajiem pasākumiem jāatbilst integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma prasībām, kas noteiktas VDAR 25. pantā.
73. Atšķirībā no 1. un 2. scenārija, kuru gadījumā pasažieri tiek autentificēti, 3.1. scenārijā pasažieri tiek identificēti (salīdzinājums 1:N), kur N ir lidostā vairāku dienu laikā gaidāmais tādu pasažieru skaits, kuri piekrituši šādai apstrādei īpašos lidostas kontrolpunktos. Tas nozīmē, ka notiktu pasažieru meklēšana centrālajā datubāzē, apstrādājot katru iegūto biometrisko paraugu, lai pārbaudītu, vai tas atbilst sistēmai zināmai personai. Atšķirībā no 2. scenārija, 3.1. scenārijā atslēgas atrodas ne tikai pie pasažieriem. Līdz ar to šajā scenārijā pasažieriem ir ievērojami mazāka kontrole pār saviem biometriskajiem datiem. Tāpēc šāda apstrāde, kā ierosināts 3.1. scenārijā, nevar būt saderīga ar integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma prasībām, kas noteiktas VDAR 25. pantā.
74. Saistībā ar VDAR 25. pantu pārziņiem būtu jāņem vērā apstrādes nolūkiem nepieciešamo personas datu veidi, kategorijas un detalizācijas pakāpe¹⁰³. Izdarot izvēles saistībā ar izstrādi, būtu jāņem vērā paaugstinātais risks attiecībā uz datu minimizēšanas, integritātes un konfidencialitātes un glabāšanas ierobežojuma principiem, vācot lielu daudzumu detalizētu personas datu, un tas jāsalīdzina ar samazinātu risku, kas saistīts ar mazāka datu apjoma un/vai mazāk detalizētas informācijas vākšanu par datu subjektiem. Jebkurā gadījumā noklusējuma iestatījumā nebūtu jāiekļauj tādu personas datu vākšana, kas nav vajadzīgi konkrētajā apstrādes nolūkā. Citiem vārdiem sakot, ja konkrētas personas datu kategorijas nav vajadzīgas vai ja nav vajadzīgi detalizēti dati, jo pietiek ar mazāk detalizētiem datiem, tad papildu personas dati nebūtu jāvāc. Ja šajā gadījumā to pašu mērķi varētu sasniegt ar citu apstrādi un ja tā ir pieejama saskaņā ar 3.1. scenārijā aprakstītajiem noteikumiem, sejas atpazīšanas tehnoloģija nav jāizmanto.
75. Saistībā ar VDAR 25. pantu galvenais integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma elements ir datu subjekta autonomija. Jo īpaši datu subjektam būtu jāpiešķir vislielākā iespējamā autonomija, lai noteiktu, kā tiek izmantoti tā personas dati, kā arī attiecībā uz minētās izmantošanas vai apstrādes tvērumu un nosacījumiem¹⁰⁴. 1. scenārijā datu subjektam būtu

¹⁰² Kā aprakstīts 64.–67. punktā iepriekš tekstā.

¹⁰³ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 49. punkts.

¹⁰⁴ EDAK Pamatnostādnes 4/2019 par 25. pantu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, 70. punkts. VDAR 7. apsvērumā ir precizēts, ka “[f]iziskām personām būtu jāspēj kontrolēt savus personas datus”.

autonomija un kontrole attiecībā uz tā biometrisko veidņu izmantošanu, atklāšanu un dzēšanu, un 2. scenārijā datu subjekts saglabātu noteiktu kontroli pār tā biometriskās veidnes atklāšanu, jo šifrēšanas atslēga / slepenā parole atrastos pie šīs personas. Tomēr 3.1. scenārijā datu subjekts ir pilnībā atkarīgs no pārziņa izdarītās izvēles attiecībā uz tā biometrisko datu apstrādi, un tāpēc tam nav tiešas kontroles pār tā biometriskās veidnes izmantošanu.

76. Attiecībā uz saderību ar VDAR 25. pantu un jo īpaši, lai izpildītu prasību par datu minimizēšanu, 3.1. scenārijā paredzētā apstrāde nevar atbilst nepieciešamības principam. Kolēģija uzskata, ka līdzīgu rezultātu attiecībā uz pasažieru plūsmas racionalizēšanu lidostās var panākt, mazāk iejaucoties privātuma aizsardzībā. Piemēram, to var panākt, neizmantojot biometriskos datus (lai gan šādā gadījumā lietotāja pieredze būtu citāda, jo varētu būt nepieciešams ilgāks laiks, lai uzrādītu iekāpšanas karti un vajadzības gadījumā oficiālus identifikācijas dokumentus). Turklāt citi risinājumi, jo īpaši tie, kuru pamatā ir biometrisko datu glabāšana vietējā makā personas ierīcē vai kuru gadījumā dati ir jāšifrē ar konkrētu atslēgu, kas tiek glabāta personas ierīcē, ļauj sasniegt mērķus veidā, kas mazāk ietekmē privātumu.
77. Attiecībā uz proporcionalitātes principu jānorāda, ka 3.1. scenārijā paredzētā apstrāde radītu tādus riskus datu subjektu tiesībām, kurus, ņemot vērā esošo progresu līmeni, paredzētās garantijas nekādi nemazinātu. Šķiet, ka negatīvās ietekmes uz datu subjektu pamattiesībām un brīvībām risks, ko varētu radīt datu aizsardzības pārkāpums centralizētā datubāzē, kur atrodas liela personu skaita biimetriskie dati, ir lielāks par paredzamo ieguvumu no apstrādes, jo šāds ieguvums ir salīdzinoši neliels, t. i., neliels ērtības un pārbaudes ātruma palielinājums. Tādējādi ar to nevar pamatot šo pasākumu izteikti ierobežojošo ietekmi attiecībā uz personu pamattiesībām un brīvībām, un 3.1. scenārijā paredzētā apstrāde neatbilst proporcionalitātes principam.
78. Atbildot uz 2.2.1. jautājumu, kolēģija, ņemot vērā šos apsvērumus, secina, ka tad, ja apstrāde tiek veikta ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās, 3.1. scenārijā paredzētā apstrāde:
- **nevar būt saderīga ar VDAR 25. pantu;**
 - **neatbilstu VDAR 5. panta 1. punkta f) apakšpunktam un 32. pantam, ja pārzinis izmantotu tikai 3.1. scenārijā aprakstītos pasākumus.**

3.2.3.2 3.2. scenārijs – centralizēta glabāšana mākonī aviosabiedrības kontrolē

Scenārija apraksts

79. 3.2. scenārijā pasažieru reģistrētā biometriskā veidne tiek glabāta mākonī aviosabiedrības vai tās mākoņpakalpojumu sniedzēja (datu apstrādātāja) kontrolē. Pieprasījumā ir norādīts, ka mākoņpakalpojumu sniedzējs atradīsies EEZ¹⁰⁵. Šajā gadījumā pasažieru datus šifrē, bet atšifrē lietošanas laikā (piemēram, kad tiek veikta salīdzināšana), un atslēgas kontrolē aviosabiedrība vai tās mākoņpakalpojuma datu apstrādātājs. Pasažieru biometriskos datus izmanto pasažieru identifikācijai (salīdzinājums 1:N), kur maksimālā N vērtība var būt aviosabiedrības kopējais klientu skaits¹⁰⁶.
80. Līdzīgi kā 1., 2. un 3.1. scenārija gadījumā, arī šajā gadījumā pasažieriem vispirms ir jāreģistrējas. Tomēr 3.2. scenārijā pasažieru reģistrācija notiek vienu reizi un ir spēkā, kamēr vien klientam ir konts aviosabiedrībā. Reģistrācija notiek attālināti atbilstošā identitātes garantijas līmenī (piemēram, eIDAS atbilstošā pārlicības līmenī) vai lidostas termināļos. Biometrisko datu salīdzināšana tiek veikta tikai tad, ja pasažieri ierodas iepriekš noteiktos lidostas kontrolpunktos, bet pati datu apstrāde notiek mākonī.
81. Lidostā pasažieri iziet cauri īpašām kontroles iekārtām, kas aprīkotas ar kameru. Pasažieru biometriskos datus ar pieprasījumu nosūta uz aviosabiedrības mākoņserveri, kur šos datus salīdzina ar centrālo datubāzi. Tādējādi var identificēt pasažieri, kā arī pārbaudīt, vai viņš patiešām ir reģistrēts izlidojošajam lidojumam (vai lidojumam, kurā notiek iekāpšana, ja kontrole tiek veikta iekāpšanas brīdī).
82. Atbilstošos rezultātus, iespējams, var darīt pieejamus vairākiem lidostu ekspluatantiem, ja aviosabiedrībai ir īpašs terminālis vai piekļuve lidostas kopējai informācijas sistēmas infrastruktūrai. Atkarībā no kontrolpunkta to datu apjomu, kas nosūtīti atpakaļ kontrolpunktā esošajam pārbaudītājam, kas veicis pieprasījumu, var samazināt līdz minimumam, piemēram, sūtot "jā/nē atbildi" vai pašu atbilstošo rezultātu, ja tas ir vajadzīgs. Šajā gadījumā kontrolpunktā esošajam pārbaudītājam ir zināms tikai pieprasījuma rezultāts, ko tas izmanto.
83. Veidnes glabāšanas laiku nosaka aviosabiedrība, un tas var būt tik ilgs, cik vien ilgi klientam ir konts aviosabiedrībā.

EDAK novērtējums

84. Apsvērumi, ko kolēģija jau ir paudusi saistībā ar 3.1. scenāriju¹⁰⁷, attiecas arī uz šo scenāriju.
85. Attiecībā uz drošības principu un prasībām (VDAR 5. panta 1. punkta f) apakšpunkts un 32. pants) jānorāda, ka 3.2. scenārijā paredzētā apstrāde tiek veikta mākonī, un vairākām struktūrām, tostarp, iespējams, ārpus EEZ esošiem pakalpojumu sniedzējiem, varētu būt piekļuve šādiem datiem pat tad,

¹⁰⁵ FR UI paskaidroja, ka šis ir ilustratīvs variants un ka varētu paredzēt arī mākoņpakalpojumu sniedzējus, kas neatrodas EEZ. Turklāt varētu paredzēt arī citus uzglabāšanas risinājumus (piemēram, neizmantojot mākonī).

¹⁰⁶ FR UI paskaidroja, ka šis ir ilustratīvs variants un ka ir risinājums, saskaņā ar kuru biometriskos datus katru reizi nosūta pirms lidojuma.

¹⁰⁷ 68.–77. punkts iepriekš tekstā.

ja dati tiek glabāti EEZ¹⁰⁸. Šāda arhitektūra ir saistīta ar iespējamu risku, kas attiecināms uz personas datu nosūtīšanu uz trešām valstīm. Turklāt, lai gan pasažieru dati ir šifrēti, tos lietošanas laikā atšifrē (t. i. tad, kad tiek veikta salīdzināšana), savukārt atslēgas kontrolē aviosabiedrība vai tās mākoņpakalpojuma datu apstrādātājs. Šāda glabāšana var vēl vairāk palielināt drošības riskam pakļauto datu daļu.

86. Tāpēc attiecībā uz saderību ar VDAR 5. panta 1. punkta f) apakšpunktu un 32. pantu 3.2. scenārijā¹⁰⁹ paredzētie pasākumi, ņemot vērā jaunākos sasniegumus, nav pietiekami, lai nodrošinātu riskam atbilstošu drošības līmeni. Pamatojoties uz minēto, 3.2. scenārijā paredzētā apstrāde neatbilstu VDAR 5. panta 1. punkta f) apakšpunktam un 32. pantam, ja pārzinis izmantotu tikai ar šos pasākumus.
87. Turklāt saskaņā ar 3.2. scenāriju¹¹⁰ datus varētu glabāt ievērojamu laiku (t. i., pat tik ilgi, cik vien ilgi datu subjektam ir konts aviosabiedrībā). Šāds glabāšanas ilgums pakļauj datus augstākam konfidencialitātes un integritātes pārkāpuma riskam, un šķietami ir ilgāks par to, kas ir absolūti nepieciešams un samērīgs apstrādes nolūkos. Kolēģija norāda, ka datu glabāšanas periods pats par sevi nav izšķirošs faktors, lai noteiktu minētās arhitektūras vispārējo saderību ar VDAR, jo datu pārziņi to var mainīt. Tomēr, pamatojoties uz kolēģijai pieejamo informāciju, kas ietverta 3.2. scenārija aprakstā, šim ilgajam glabāšanas periodam nav pietiekama pamatojuma un nav acīmredzamu pasākumu, lai mazinātu risku personām. Pamatojoties uz minēto, ierosinātais glabāšanas periods būtu ilgāks nekā nepieciešams saskaņā ar VDAR 5. panta 1. punkta e) apakšpunktā noteikto uzglabāšanas ierobežojuma principu.
88. Jebkurā gadījumā 3.2. scenārijā ierosinātie pasākumi nevar izpildīt integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma prasības, kas noteiktas VDAR 25. pantā. 3.2. scenārija gadījumā pasažieru reģistrētās biometriskās veidnes tiek glabātas mākonī aviosabiedrības vai tās mākoņpakalpojumu sniedzēja (datu apstrādātāja) kontrolē. Kā aprakstīts iepriekš, šiem datiem potenciāli varētu piekļūt vairākas struktūras. Turklāt pasažieru biometriskos datus izmanto pasažieru identifikācijai (salīdzinājums 1:N), kur maksimālā N vērtība var būt aviosabiedrības kopējais lietotāju / klientu skaits. Šāda metode ietver personas atrašanu personu grupā centrālajā datubāzē, apstrādājot katru uztverto seju, lai pārbaudītu, vai tā atbilst sistēmai zināmai personai. Atšķirībā no 3.1. scenārija 3.2. scenārijā paredzēto salīdzināšanu varētu veikt daudz plašākā mērogā, jo šajā gadījumā kritērijs ir aviosabiedrības kopējais klientu skaits, bet 3.1. scenārijā ir iekļauts tikai tāds pasažieru skaits, kas paredzams vairāku dienu laikā.
89. Turklāt attiecībā uz saderību ar VDAR 25. pantu un jo īpaši, lai izpildītu prasību par datu minimizēšanu, 3.2. scenārijā paredzētā apstrāde nevar atbilst nepieciešamības principam. Kolēģija uzskata, ka līdzīgu rezultātu, racionalizējot pasažieru plūsmu lidostās, varētu sasniegt ar citiem mazāk ierobežojošiem pasākumiem, piemēram, neizmantojot biometriskos datus, lai gan lietotāja pieredze šādā gadījumā būtu atšķirīga, jo personas apliecības un iekāpšanas kartes uzrādīšana varētu prasīt vairāk laika. Turklāt citi risinājumi, jo īpaši tie, kuru pamatā ir biometrisko datu glabāšana vietējā makā personas ierīcē vai

¹⁰⁸ EDAK 2022. gada koordinētā izpildes darbība attiecībā uz mākoņpakalpojumu izmantošanu publiskajā sektorā, 2023. gada 17. janvāris, 19. lpp.

¹⁰⁹ Skatīt 79.–83. punktu iepriekš tekstā.

¹¹⁰ Skatīt 83. punktu iepriekš tekstā.

kuru gadījumā dati ir jāšifrē ar konkrētu atslēgu, kas tiek glabāta personas ierīcē, ļauj pārzinim sasniegt mērķus veidā, kas mazāk ietekmē privātumu.

90. Attiecībā uz proporcionalitātes principu jānorāda, ka 3.2. scenārijā paredzētā apstrāde radītu tādu riskus datu subjektu tiesībām, kurus paredzētās garantijas nekādi nemazinātu. Šķiet, ka negatīvā ietekme uz datu subjektu pamattiesībām un brīvībām, ko radītu datu aizsardzības pārkāpums centralizētā datubāzē, kur mākonī tiek glabāti liela personu skaita biometriskie dati, ir lielāka par paredzamo ieguvumu no apstrādes, jo šāds ieguvums ir salīdzinoši neliels, t. i., neliels ērtības un pārbaudi ātruma palielinājums. Tādējādi ar to nevar pamatot šo pasākumu izteikti ierobežojošo ietekmi attiecībā uz personu pamattiesībām un brīvībām, un 3.2. scenārijā paredzēto apstrādi nevar uzskatīt par proporcionālu.
91. Atbildot uz 2.3.1. jautājumu, kolēģija, ņemot vērā šos apsvērumus, secina, ka tad, ja apstrāde tiek veikta ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās, 3.2. scenārijā paredzētā apstrāde:
- **nevar būt saderīga ar VDAR 25. pantu;**
 - **neatbilstu VDAR 5. panta 1. punkta f) apakšpunktam un 32. pantam**, ja pārzinis izmantotu tikai 3.2. scenārijā aprakstītos pasākumus;
 - **neatbilstu VDAR 5. panta 1. punkta e) apakšpunktam**, jo, pamatojoties uz kolēģijai pieejamo informāciju, nav pietiekama 3.2. scenārijā paredzētā glabāšanas perioda pamatojuma. Lai ievērotu VDAR 5. panta 1. punkta e) apakšpunktā noteikto glabāšanas ierobežojuma principu, pārzinim būtu jāpierāda, ka personas dati netiek glabāti ilgāk, kā tas nepieciešams nolūkiem, kādos tos apstrādā.

4 SECINĀJUMI

92. Attiecībā uz 1.1. jautājumu, pamatojoties uz FR UI lūgumu sniegt atzinumu par atbilstību VDAR 5. panta 1. punkta f) apakšpunkta, 25. un 32. panta prasībām un pamatojoties uz iepriekš izklāstīto analīzi, kolēģija secina, ka:
93. sejas atpazīšanas tehnoloģijas lietošanu, lai veiktu autentifikāciju, izmantojot biometriskus datus, ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās (drošības kontrolpunkti, bagāžas nodošanas punkti, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpai) principā varētu uzskatīt par saderīgu ar integritātes un konfidencialitātes principiem, kas noteikti VDAR 5. panta 1. punkta f) apakšpunktā, 25. un 32. pantā, glabāšanas arhitektūras gadījumā, ja katra pasažiera reģistrētā biometriskā veidne tiek uzglabāta lokāli viņa individuālajā ierīcē un tikai un vienīgi viņa kontrolē, ja tiek īstenotas atbilstošas garantijas, kā aprakstīts 46. punktā.
94. Attiecībā uz 2.1.1. jautājumu, pamatojoties uz FR UI lūgumu sniegt atzinumu par atbilstību VDAR 5. panta 1. punkta e) un f) apakšpunkta un 25. un 32. panta prasībām un pamatojoties uz iepriekš izklāstīto analīzi, kolēģija secina, ka:
95. sejas atpazīšanas tehnoloģijas lietošanu, lai veiktu autentificēšanu, izmantojot biometriskus datus, ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās (drošības kontrolpunkti, bagāžas nodošanas punkti, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpai) principā varētu uzskatīt par saderīgu ar glabāšanas ierobežojuma principu, kas noteikts 5. panta 1. punkta e) apakšpunktā, un integritātes un konfidencialitātes principiem, kas noteikti VDAR 5. panta 1. punkta f) apakšpunktā un 25. un

32. pantā, centralizētas glabāšanas arhitektūras gadījumā, ja katra pasažiera reģistrētā un šifrētā biometriskā veidne tiek glabāta lidostas centrālajā datubāzē lidostas ekspluatanta kontrolē, atslēgai / slepenajai parolei atrodas tikai pie attiecīgās personas, ja tiek īstenotas atbilstošas garantijas, kā aprakstīts 60. punktā.

96. Attiecībā uz 2.2.1. jautājumu, pamatojoties uz FR UI lūgumu sniegt atzinumu par atbilstību VDAR 5. panta 1. punkta f) apakšpunkta, 25. un 32. panta prasībām un pamatojoties uz iepriekš izklāstīto analīzi, kolēģija secina, ka:
97. sejas atpazīšanas tehnoloģijas lietošana, lai veiktu identificēšanu, izmantojot biometriskus datus, ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās (drošības kontrolpunkti, bagāžas nodošanas punkti, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpai) centralizētas glabāšanas arhitektūras gadījumā, ja pasažieru reģistrētās biometriskās veidnes nav šifrētas ar atslēgu / slepenu paroli, kas atrodas tikai pie katra pasažiera, ja šādas veidnes tiek glabātas datubāzē lidostā (lidostas ekspluatanta kontrolē), nevar būt saderīga ar VDAR 25. pantu. Šāda apstrāde arī neatbilstu VDAR 5. panta 1. punkta f) apakšpunktā un 32. pantā noteiktajiem integritātes un konfidencialitātes principiem, ja pārzinis izmantotu tikai 3.1. scenārijā aprakstītos pasākumus.
98. Attiecībā uz 2.3.1. jautājumu, pamatojoties uz FR UI lūgumu sniegt atzinumu par atbilstību VDAR 5. panta 1. punkta f) apakšpunkta, 25. un 32. panta prasībām un pamatojoties uz iepriekš izklāstīto analīzi, kolēģija secina, ka:
99. sejas atpazīšanas tehnoloģijas lietošana, lai veiktu identificēšanu, izmantojot biometriskus datus, ar konkrētu mērķi racionalizēt pasažieru plūsmu lidostās (drošības kontrolpunkti, bagāžas nodošanas punkti, iekāpšanas laikā un piekļūstot pasažieru atpūtas telpai) centralizētas glabāšanas arhitektūras gadījumā, ja pasažieru reģistrētās biometriskās veidnes nav šifrētas ar atslēgu / slepenu paroli, kas atrodas tikai pie katra pasažiera, ja šādas veidnes tiek glabātas mākonī (aviosabiedrības kontrolē), nevar būt saderīga ar VDAR 25. pantu. Turklāt šāda apstrāde neatbilstu VDAR 5. panta 1. punkta f) apakšpunktā un 32. pantā noteiktajiem integritātes un konfidencialitātes principiem, ja pārzinis izmantotu tikai 3.2. scenārijā aprakstītos pasākumus. Visbeidzot, pamatojoties uz 3.2. scenārija aprakstu un kolēģijai pieejamo informāciju, apstrāde neatbilstu VDAR 5. panta 1. punkta e) apakšpunktā noteiktajam glabāšanas ierobežojuma principam.

Eiropas Datu aizsardzības kolēģijas vārdā –

priekšsēdētāja

(Anu Talus)