Становище на Комитета (член 64)

Становище 11/2024 относно използването на лицево разпознаване за рационализиране на пътникопотока на летищата (съвместимост с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД)

Версия 1.1

Приети на 23 май 2024 г.

Приети

Версия 1.1	28 май 2024 г.	Граматически корекции в резюмето (страници 3 и 4) и в точки 77 и 90 от становището
Версия 1.0	23 май 2024 г.	Приемане на становището

Резюме

Френският надзорен орган поиска от Европейския комитет по защита на данните да изготви становище относно използването на технологии за лицево разпознаване от страна на летищните оператори и авиокомпаниите за идентифициране или проверка на самоличността на пътниците с помощта на биометрични данни с цел да се рационализира пътникопотока на летищата.

Като предварителна бележка Комитетът припомня, че използването на биометрични данни, и по-специално на технологии за лицево разпознаване, води до повишени рискове за правата и свободите на субектите на данни. Става въпрос за обработването на биометрични данни, които се ползват от специална защита съгласно член 9 от ОРЗД. Преди да прибегнат към използването на такива технологии, дори ако те се считат за особено ефективни, администраторите следва да оценят въздействието върху основните права и свободи на физическите лица и да преценят дали законната цел на обработването може да се постигне със средства, които представляват по-малка намеса.

В съответствие с искането обхватът на настоящото становище е ограничен до съвместимостта на обработването с **член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД** с **конкретната цел да се рационализира пътникопотока на летищата** в четири конкретни точки, а именно пунктовете за проверка за сигурност, при оставянето на багаж, отвеждането към самолета и при влизането в салоните за пътници. Настоящото становище не включва пълен и изчерпателен анализ на съвместимостта с ОРЗД на съответния администратор или администратори във всеки отделен случай, както и на назначения от тях обработващ или обработващи лични данни, ако е приложимо. Поради това настоящото становище не засяга правния и техническия анализ на отделни случаи въз основа на конкретното предвидено обработване на данни от администратора, както и на свързаните с това и обстоятелства. Освен това анализът на приложимото правно основание не попада в обхвата на отправените до Комитета въпроси, посочени в искането, поради което в настоящото становище не се разглежда валидността на съгласието за това обработване в съответствие с членове 6, 7 и 9 от ОРЗД. В допълнение, становището не засяга ограниченията по отношение на използването на биометрични данни, определени в законодателството на държавите членки.

В настоящото становище Комитетът оценява дали обработването е в съответствие с горепосочените разпоредби на ОРЗД в рамките на **четири конкретни сценария**.

Първият сценарий е свързан със съхраняването на регистриран биометричен образец, с които лицето разполага, например в индивидуалното му устройство, и под негов изключителен контрол, с цел удостоверяване на автентичността (сравнение 1:1) на пътника при преминаването му през горепосочените пунктове на летището.

Комитетът заключава, че би могло да се счита, че избраните мерки отговарят на принципа за необходимост, ако администраторът може да докаже, че няма алтернативни решения, които представляват по-малка намеса и които биха могли да постигнат същата цел със същата ефективност. Освен това, намесата в резултат на обработването може да бъде неутрализирана от активното участие на пътниците, тъй като биометричният им образец се съхранява единствено от тях и под изключителния им контрол, например в индивидуалните им устройства, и данните им се заличават скоро след приключване на съпоставянето. На тази основа Комитетът заключава, че обработването, предвидено в първия сценарий, **принципно би могло да се счита**

за съвместимо с член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД, при условие че се прилагат подходящи гаранции.

Комитетът определи гаранциите, които следва да се прилагат като минимум, ако бъде възприето решение, подобно на първия сценарий.

Вторият сценарий е свързан с централизирано съхраняване в рамките на летището на регистриран биометричен образец в криптирана форма, ключът/тайната за който са достъпни единствено за пътника. Това дава възможност за удостоверяване на самоличността на пътника (сравнение 1:1) при преминаването му през горепосочените пунктове на летището. Регистрацията е валидна за определен период, който може да варира например от една година след последния полет до датата на изтичане на валидността на паспорта.

Комитетът заключава, че би могло да се счита, че обработването отговаря на принципа за необходимост, ако администраторът може да докаже, че няма алтернативни решения, които представляват по-малка намеса и които биха могли да постигнат същата цел със същата ефективност. Освен това намесата в резултат на обработването може да бъде неутрализирана от активното участие на пътника, тъй като ключът/тайната за криптираните му биометрични данни се държат под негов изключителен контрол. Ако се приеме, че администраторът прилага подходящи гаранции, рисковете за сигурността, произтичащи от използването на централизирана база данни в този сценарий, биха могли да се ограничат, а отрицателното въздействие върху основните права и свободи на субектите на данни биха могли да се считат за пропорционални на очакваните ползи. Що се отнася до принципа за ограничение на съхранението, на Комитета не е предоставена информация, която да обоснове дълъг период на съхранение. За да се постигне съвместимост с член 5, параграф 1, буква д) от ОРЗД в този сценарий, администраторите следва да могат да обосноват защо предвиденият период на съхранение е необходим за целите в конкретните случаи. Комитетът препоръчва администраторите да предвиждат най-краткия възможен период на съхранение, като същевременно предлагат на пътниците възможност да определят предпочитания от тях период . На тази основа Комитетът заключава, че обработването, предвидено в сценарий 2, **принципно би могло да се счита за съвместимо с член 5, параграф 1, буква д), член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД**, при условие че се прилагат подходящи гаранции.

Комитетът определи гаранциите, които следва да се прилагат като минимум, ако бъде възприето решение, подобно на втория сценарий.

Третият сценарий е свързан с централизирано съхранение в рамките на летището на регистриран биометричен образец в криптирана форма под контрола на летищния оператор. Това дава възможност за идентифициране на пътниците (сравнение 1:N) при преминаването им през горепосочените пунктове на летището. Периодът на съхранение в този сценарий обикновено е 48 часа и данните се заличават след заминаването на самолета.

Тъй като идентификационните и биометричните данни се съхраняват в централна база данни, ако поверителността на базата данни бъде компрометирана, това може в последствие да доведе до достъп до целия набор от данни и би могло да създаде условия за неразрешено или неправомерно идентифициране на пътниците при други обстоятелства. Централизираната архитектура за съхранение под контрола на летищния оператор също така означава, че пътниците в по-голяма степен губят контрол върху своите данни. Комитетът счита, че подобен резултат от гледна точка на рационализирането на пътникопотока на летищата може да бъде постигнат по начин, който представлява по-малка намеса, и че отрицателното въздействие

върху основните права и свободи на субектите на данни в резултат на нарушение на сигурността на данните в централизирана база данни, съдържаща биометрични данни, изглежда надхвърля очакваните ползи от обработването. Поради това обработването не отговаря на принципите на необходимост и пропорционалност. На тази основа Комитетът заключава, че обработването, предвидено в третия сценарий, **не може да бъде съвместимо с член 25 от ОРЗД**. Освен това то **не би отговаряло на член 5, параграф 1, буква е) и член 32 от ОРЗД**, ако администраторът се ограничи до описаните в този сценарий мерки.

Четвъртият сценарий се отнася до централизираното съхранение на регистриран биометричен образец в криптирана форма „в облак“ под контрола на авиокомпанията или доставчика ѝ на компютърни облачни услуги. Това дава възможност за идентифициране на пътниците (сравнение 1:N) при преминаването им през горепосочените пунктове на летището. Периодът на съхранение в този сценарий потенциално може да отговаря на целия период, в който клиентът разполага с профил в авиокомпанията.

Тъй като идентификационните и биометричните данни се съхраняват в централна база данни в облака, множество субекти биха могли да разполагат с достъп до тях, включително евентуално доставчици от държави извън ЕИП. Данните на пътниците се декриптират, когато се използват, а ключовете са под контрола на авиокомпанията или назначените от нея обработващи лични данни, което би могло да увеличи мащаба на разкриване на информация, което има отношение към сигурността. Такава централизирана архитектура за съхранение също така означава, че пътниците в по-голяма степен губят контрол върху своите данни. Освен това данните биха могли да се съхраняват за значителен период от време, което ги излага на по-големи рискове от нарушение на сигурността и изглежда надхвърля абсолютно необходимото и пропорционалното за целите на обработването, освен ако не се предприемат допълнителни видими мерки за ограничаване на рисковете за лицата.

Комитетът счита, че подобен резултат от гледна точка на рационализирането на пътникопотока на летищата може да бъде постигнат по начин, който представлява по-малка намеса, и че отрицателното въздействие върху основните права и свободи на субектите на данни, което би могло да възникне в резултат на нарушение на сигурността на данните в централизирана база данни, съдържаща биометрични данни, изглежда надхвърля очакваните ползи от обработването. Поради това обработването не отговаря на принципите на необходимост и пропорционалност. На тази основа Комитетът заключава, че обработването, предвидено в четвъртия сценарий, **не може да бъде съвместимо с член 25 от ОРЗД**. Освен това въз основа на информацията, с която разполага Комитетът, то **не би отговаряло на член 5, параграф 1, буква д) от ОРЗД**, както и **не би отговаряло на член 5, параграф 1, буква е) и член 32 от ОРЗД**, ако администраторът се ограничи до описаните в този сценарий мерки.

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 63 и член 64, параграф 2 от Регламент 2016/679/ЕС на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „**ОРЗД**“),

като взе предвид Споразумението за ЕИП, и по-специално приложение XI и Протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.[1],

като взе предвид член 10 и член 22 от Правилника за дейността на Европейския комитет по защита на данните (наричан по-нататък „**Комитетът**“ или „**ЕКЗД**“) (наричан по-нататък „**ПД на ЕКЗД**“),

като има предвид, че:

(1) Основната роля на Комитета е да гарантира последователното прилагане на ОРЗД в Европейското икономическо пространство (наричано по-нататък „**ЕИП**“). В член 64, параграф 2 от ОРЗД се предвижда, че всеки надзорен орган (наричан по-нататък „**НО**“), председателят на Комитета или на Европейската комисия може да поиска разглеждането на въпрос с общо приложение или с последици в повече от една държава — членка на ЕИП, от Комитета с цел получаване на становище.

(2) Становището на Комитета се приема в съответствие с член 64, параграф 3 от ОРЗД във връзка с член 10, параграф 2 от ПД на ЕКЗД в срок от осем седмици, считано от момента, в който председателят и компетентният НО решат, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици с оглед на сложността на въпроса,

прие следното становище:

1 ВЪВЕДЕНИЕ

1.1 Кратко изложение на фактите

1. На 16 февруари 2024 г. Френският надзорен орган (наричан по-нататък „**Френския НО**“) поиска от Комитета да изготви становище относно съвместимостта с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД на използването на технологии за лицево разпознаване от страна на летищните оператори и авиокомпаниите за идентифициране и проверка на самоличността на

[1] Позоваванията на „**държави членки**“ в настоящото становище следва да се разбират като позовавания на „държавите — членки на ЕИП“. Позоваванията на „Съюза“ или „ЕС“ в настоящото становище следва да се разбират като позовавания на „ЕИП“.

пътниците с помощта на биометрични данни[2] с цел да се рационализира пътникопотока на пунктовете за проверка за сигурност на летищата[3], при оставянето на багаж, отвеждането към самолета и при влизането в салоните за пътници (с изключение на граничния контрол и проверките, извършвани от безмитните магазини) (наричано по-нататък „**искането**“). Френският НО приложи към искането си описание на типични случаи на употреба (приложение I).

2. В искането си Френският НО отбелязва, че моделите, които понастоящем се изпитват в няколко летища в ЕС, варират в отделните държави членки, което евентуално поражда риск от разминаване в тълкуването сред отделните НО, както и риск от пораждане на различни ефекти за основните права и свободи на субектите на данни в ЕС[4].

3. Комитетът счита, че с цел да предостави отговор на искането трябва да бъде отговорено на следните въпроси:

4. **Въпрос 1**:

1.1. Може ли използването на технологии за лицево разпознаване за проверка на самоличността с помощта на биометрични данни **с конкретната цел да се рационализира пътникопотока на летищата** (пунктове за проверка за сигурност, при оставянето на багаж, отвеждането към самолета и влизането в салоните за пътници) да е съвместимо с **член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД** в случай на архитектура за съхранение, при която биометричният образец на всеки пътник се съхранява **единствено от физическото лице**, например на място в индивидуалното му устройство, под негов изключителен контрол?

1.2. Ако такова обработване бъде счетено за съвместимо с горепосочените разпоредби, какви минимални подходящи гаранции биха били необходими с оглед на членове 25 и 32 от ОРЗД?

Въпрос 2:

2.1. Може ли използването на технологии за лицево разпознаване за проверка на самоличността с помощта на биометрични данни **с конкретната цел да се рационализира пътникопотока на летищата** (пунктове за проверка за сигурност, при оставянето на багаж, отвеждането към самолета и влизането в салоните за пътници) да е съвместимо с **член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД** в случай на **централизирана** архитектура за съхранение, при която биометричният образец на всеки пътник се съхранява в централна база данни:

2.1.1. В централна база данни в рамките на летището, под контрола на летищния оператор, в криптирана форма, ключът/тайната за която са достъпни единствено за

[2] В контекста на настоящото становище „**пътник**“ означава субект на данни, чиито лични данни се обработват за конкретната цел, описана в настоящото становище. По-нататък в настоящото становище термините „пътник“ и „лице“ се употребяват взаимозаменяемо.

[3] За целите на настоящото становище „**пунктове за проверка за сигурност на летищата**“ означава проверките за сигурност, извършвани под отговорността на летищния оператор, през които пътниците трябва да преминат, така че от залата за заминаващи да влязат в зоната за качване на борда или изхода за отвеждане на борда.

[4] Искане, стр. 1.

физическото лице (например в мобилния телефон на лицето), с цел проверка на самоличността?

2.1.2. Ако такова обработване бъде счетено за съвместимо, какви минимални подходящи гаранции биха били необходими с оглед на членове 25 и 32 от ОРЗД?

2.2.1. В централна база данни в рамките на летището, под контрола на летищния оператор, в криптирана форма, като ключовете се държат от летищния оператор, с цел идентифициране?

2.2.2. Ако такова обработване бъде счетено за съвместимо, какви минимални подходящи гаранции биха били необходими с оглед на членове 25 и 32 от ОРЗД?

2.3.1. В облака, под контрола на авиокомпанията или доставчика ѝ на услуги (обработващия лични данни), в криптирана форма, като ключовете се държат от авиокомпанията или доставчика ѝ на услуги, с цел идентифициране?

2.3.2. Ако такова обработване бъде счетено за съвместимо, какви минимални подходящи гаранции биха били необходими с оглед на членове 25 и 32 от ОРЗД?

5. След като Френския НО счете досието за пълно на 16 февруари 2024 г., а председателят на Комитета го счете за пълно на 23 февруари 2024 г., то беше разпространено от секретариата на 23 февруари 2024 г. В съответствие с член 64, параграф 3 от ОРЗД във връзка с член 10, параграф 2 от ПД на ЕКЗД председателят на Комитета реши да удължи осемседмичния срок за приемане по подразбиране с още шест седмици поради сложността на предмета.

1.2 Допустимост на искането за становище по член 64, параграф 2 от ОРЗД

6. В член 64, параграф 2 от ОРЗД се предвижда по-специално, че всеки НО може да поиска разглеждането от Комитета на въпрос с общо приложение или с последици в повече от една държава членка с цел получаване на становище.

7. Комитетът счита, че отправеното от Френския НО искане относно съвместимостта на използването на технологии за лицево разпознаване за идентифициране или проверка на самоличността с помощта на биометрични данни с конкретната цел да се рационализира пътникопотока на летищата е свързано с въпроси „с последици в повече от една държава членка“, защото, както е обяснено в искането[5], понастоящем на летищата в държавите членки са в ход няколко проекта и се прогнозира, че използването на такива технологии ще се увеличи през следващите години. Моделите, които понастоящем се изпитват от различни летища и авиокомпании, се различават значително между отделните държави членки, поради което е възможно да породят риск от възникването на различни ефекти в повече от една държава членка от гледна точка на защитата на личните данни.

8. Освен това Комитетът счита, че отправеното от Френския НО искане води до значими последици за прилагането на принципите, посочени в член 5, параграф 1, букви д) и е) от ОРЗД, и изискванията, приложими за администраторите съгласно член 25 от ОРЗД, както и за тези, приложими за администраторите и обработващите лични данни съгласно член 32 от ОРЗД.

[5] Искане, стр. 3.

Поради това настоящото искане се отнася до „въпрос с общо приложение“ по смисъла на член 64, параграф 2 от ОРЗД, тъй като е свързано с последователното тълкуване на принципите за ограничение на съхранението (член 5, параграф 1, буква д) от ОРЗД) и за цялостност и поверителност (член 5, параграф 1, буква е) от ОРЗД), както и с понятията за защита на данните на етапа на проектирането и по подразбиране (член 25 от ОРЗД) и за сигурност на данните (член 32 от ОРЗД), като целта е, наред с други неща, да се гарантира последователното прилагане на тези разпоредби в ЕИП.

9. Евентуалните разлики в позициите в отделните държави членки по отношение на тълкуването на член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД биха повишили риска летищните оператори и авиокомпаниите да разработват проекти за лицево разпознаване по непоследователен начин. Тъй като Френският НО доказа ясната необходимост от последователно тълкуване на тези разпоредби във връзка с технологиите за лицево разпознаване за идентифициране или проверка на самоличността на пътниците с помощта на биометрични данни с цел да се рационализира пътникопотока на летищата[6], Комитетът счита искането за мотивирано в съответствие с член 10, параграф 3 от ПД на ЕКЗД.

10. Съгласно член 64, параграф 3 от ОРЗД ЕКЗД не дава становище, ако вече е дал становище по въпроса[7]. Досега ЕКЗД не е представял отговори на въпросите, произтичащи от искането. Въпреки че в Насоки 3/2019 на ЕКЗД относно видеоустройствата[8] вече са посочени някои полезни елементи по отношение на мерките за сигурност, които следва да се прилагат към обработването на биометрични данни, в тях не се разглеждат всички аспекти във връзка с повдигнатите в искането въпроси. Освен това в наличните насоки на ЕКЗД, включително Насоки 3/2019 на ЕКЗД относно видеоустройствата, не са предвидени конкретни указания относно евентуалните елементи, които трябва да бъдат проверени във връзка с централизираното или децентрализираното съхраняване на биометрични данни за идентифициране или проверка на самоличността на пътниците с цел да се рационализира пътникопотока на летищата, както и относно съвместимостта на това обработване с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД.

11. Поради тези причини Комитетът счита, че искането е допустимо и повдигнатите в него въпроси следва да бъдат анализирани в становище, прието съгласно член 64, параграф 2 от ОРЗД.

2 ОБХВАТ И КОНТЕКСТ НА СТАНОВИЩЕТО

2.1 Обхват на становището

12. Настоящото становище се отнася единствено до съвместимостта с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД на използването на технологии за лицево разпознаване за идентифициране или проверка на самоличността с помощта на биометрични данни на пътници от страна на летищните операторите и авиокомпаниите **с конкретната цел да се рационализира**

[6] Искане, стр. 1—3.
[7] Член 64, параграф 3 от ОРЗД и член 10, параграф 4 от Правилника за дейността на ЕКЗД.
[8] Насоки 3/2019 на ЕКЗД относно обработването на лични данни чрез видеоустройства, версия 2.0, приети на 29 януари 2020 г. (наричани по-нататък „**Насоки 3/2019 на ЕКЗД относно видеоустройствата**“).

пътникопотока на летищата, а именно на пунктовете за проверка за сигурност, при оставянето на багаж, отвеждането към самолета и при влизането в салоните за пътници, съгласно искането.

13. По отношение на **обхвата на настоящото становище** Комитетът пояснява следното:

1) Обработването на лични данни в рамките на граничния контрол и на проверките, извършвани от безмитните магазини, не попада в обхвата на настоящото становище, тъй като те се извършват от администратори, които са различни от летищните оператори и авиокомпаниите.

2) Използването на технологии за лицево разпознаване, дори въз основа на сценариите, описани в раздел 3.2 по-долу, за каквито и да е други цели (включително правоприлагане) или от каквито и да е други страни, дори за сходни цели, попада извън обхвата на настоящото становище.

3) В настоящото становище се разглежда обработването на личните данни на пътници, като то не обхваща други видове субекти на данни, като например персонала на летищните оператори или на авиокомпаниите.

4) В настоящото становище се разглежда искането, както е представено от Френския НО, във връзка със съвместимостта на системата за съхранение на биометричните образци на пътниците с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД. В това отношение настоящото становище не включва пълен и изчерпателен анализ на съвместимостта с ОРЗД на съответния администратор или администратори във всеки отделен случай, както и на назначения от тях обработващ или обработващи лични данни, ако е приложимо. Това е особено важно с оглед на факта, че тези технологии водят до повишени рискове, свързани с обработването на специални категории данни в съответствие с член 9 от ОРЗД. Поради това в този документ не се засяга оценката във връзка с други разпоредби на ОРЗД по отношение на използването на технологии за лицево разпознаване, включително в конкретния сектор, обхванат от искането, или правния и технически анализ на отделни случаи, които могат да бъдат обособени предвид предвидено обработване на данни и конкретните обстоятелства на администратора.

5) В настоящото становище не се разглежда обработването на личните данни на деца, като то не засяга специфичните изисквания, които се прилагат в този случай.

6) Настоящото становище не засяга правните изисквания и допълнителните ограничения относно използването на биометрични данни, произтичащи от националните законодателства на държавите членки[9].

7) Заключенията в документа не засягат по-нататъшното развитие на технологиите.

[9] Например в член 9, параграф 4 от ОРЗД се предвижда, че държавите членки могат да запазят или да въведат допълнителни условия, включително и ограничения, по отношение на обработването на биометрични данни.

8) В становището се разглеждат четири сценария, чиито специфични характеристики са описани в раздел 3.2 по-долу. В него не се разглеждат други сценарии, дори в случай че обработването се извършва за същите цели.

14. В искането си Френския НО посочи, че обработването на биометричните данни на пътниците с цел да се рационализира пътникопотока на летищата се основава на допускането, че лицата дават своето съгласие за това обработване, което евентуално би формирало правното основание съгласно ОРЗД[10]. **Въпреки това анализът на приложимото правно основание не попада в обхвата на отправените до ЕКЗД въпроси, посочени в искането, поради което в настоящото становище не се разглежда валидността на съгласието за това обработване в съответствие с членове 6, 7 и 9 от ОРЗД.**

15. Независимо от това ЕКЗД отбелязва, че ако съответните администратори разчитат на това правно основание, те ще трябва да получат валидно изрично съгласие[11] от лицата, които желаят да използват тези услуги. Такова изрично съгласие трябва да е свободно изразено, конкретно и информирано[12], като изпълнението на тези условия се анализира поотделно във всеки случай. Това по-специално означава, че:

1) Лицата трябва да могат лесно и без никакви неудобства да оттеглят това съгласие по всяко време[13].

2) За да е свободно дадено съгласието, такова използване на технологии с помощта на биометрични данни може да се осъществява само на доброволна основа, тъй като лицата следва да могат да избират дали да използват тези услуги свободно и без никакви неудобства (като например значително по-дълго забавяне за пътниците, които не дават своето съгласие[14]), стимули, допълнителни разходи или допълнителни предимства в замяна на това[15].

3) Освен това трябва да се поиска изричното съгласие на лицата, чиито биометрични данни се обработват, дори ако не са се регистрирали за идентифициране или проверка на самоличността чрез такива средства. С други

[10] Искане, приложение I.

[11] В съответствие с член 4, точка 14 и член 9, параграф 1 от ОРЗД, както и член 9, параграф 2, буква а) от ОРЗД се забранява обработването на биометрични данни за целите единствено на идентифицирането на физическо лице, освен ако субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на Съюза или правото на държава членка се предвижда, че посочената в член 9, параграф 1 от ОРЗД забрана не може да бъде отменена от субекта на данни. Вж. също съображения 51, 52 и 53 от ОРЗД.

[12] Член 4, точка 11 и член 7 от ОРЗД.

[13] Член 7, параграф 4 от ОРЗД, също съображение 50 от ОРЗД.

[14] Това може да включва например съображения като проектирането на дадена система по такъв начин, че да се избягва създаването на социален натиск върху пътниците, които не желаят да дадат своето съгласие, като се избягва ситуация, в която този избор се отразява отрицателно на останалите пътници.

[15] Насоки 5/2020 на ЕКЗД относно съгласието в съответствие с Регламент 2016/679, версия 1.1, приети на 4 май 2020 г. (наричани по-нататък „**Насоки 5/2020 на ЕКЗД относно съгласието**“), точки 46, 48.

думи, от съществено значение е да не се сканират лицата на хората, които не са дали изрично съгласие за лицево разпознаване за предвидените цели. Това може да бъде постигнато например чрез обособяване на конкретни ленти за лицево разпознаване и осигуряване на подходящи знаци и физическо отделяне от потоците за контрол без използването на биометрични данни, за да се даде възможност за ясно определяне на тези ленти.

4) Без да се засяга въпросът дали съгласието би било приложимото правно основание за такова обработване, залегналите в член 5 от ОРЗД принципи за обработване, свързаните с необходимостта и пропорционалността, продължават да се прилагат дори когато лицата са дали изричното си съгласие за използването на биометричните им данни[16].

16. В искането се уточнява[17], че летищните оператори ще действат като администратори по отношение на обработването в пунктовете за проверка за сигурност на летищата, докато авиокомпаниите ще действат като администратори по отношение на обработването при оставянето на багажа, отвеждането към самолета и при влизането в салоните за пътници. Поради това Комитетът отбелязва, че в обработването, описано в искането, е възможно да участват различни участници и че не е оценил прилагането на ролите на (съвместен) администратор и/ обработващ лични данни в сценариите, описани по-долу в раздел 3.2 от настоящото становище. Във всеки случай съответните участници трябва да бъдат идентифицирани и отговорностите им да бъдат ясно разпределени, за да бъдат изпълнени изискванията на ОРЗД[18].

17. Освен това Комитетът отбелязва, че понастоящем в ЕС няма единно правно изискване летищните оператори и авиокомпаниите да идентифицират пътниците и да проверяват дали името на бордната карта на пътника съответства на името на документа му за самоличност във всички горепосочени пунктове за проверка[19]. Поради това всички такива изисквания са обхванати от националните законодателства, които може да варират в отделните държави членки. В някои държави членки е възможно да се изисква такава проверка за някои пунктове (например оставянето на багажа или отвеждането към самолета), докато в други понастоящем

[16] Пак там, параграф 5.
[17] Искане, приложение I.
[18] В съответствие с член 4, параграфи 7 и 8, член 5, параграф 2 и членове 24, 26, 28 и 29 от ОРЗД. Вж. също Насоки 07/2020 на ЕКЗД относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, версия 2.1, приети на 7 юли 2021 г.
[19] Съответният регламент на равнището на ЕС е Регламент за изпълнение (ЕС) 2015/1998 на Комисията от 5 ноември 2015 г. за установяване на подробни мерки за прилагането на общите основни стандарти за сигурност във въздухоплаването. В този регламент обаче не са разгледани проверките на официалните документи за самоличност в пунктовете за проверка на летищата и държавите членки разполагат с право на преценка как да регламентират този въпрос на национално равнище.

не се изискват такива проверки[20]. Наличието на правни задължения за проверка на самоличността на пътниците оказва пряко въздействие върху различните практики на летищата.

18. Като последица от това, когато в такива ситуации **не се изисква проверка на самоличността на пътниците с официален документ за самоличност, не следва да се извършва проверка с помощта на биометрични данни, тъй като това би довело до прекомерно обработване на данни, защото предполага обработването на допълнителни данни в сравнение с настоящата ситуация и би надхвърлило необходимото за съответната цел, в нарушение на принципа за свеждане на данните до минимум, посочен в член 5, параграф 1, буква в) от ОРЗД.** Това съображение следва да се има предвид при разглеждането на всички сценарии, описани по-долу в раздел 3.2 от настоящото становище.

2.2 Основни понятия

19. За да отговаря на критериите за биометрични данни съгласно член 4, точка 14 от ОРЗД[21], дейността по обработване на необработени данни като физически, физиологични или поведенчески характеристики на дадено физическо лице трябва да включва измерване на тези характеристики, тъй като биометричните данни се получават в резултат на такива измервания[22].

20. Посредством използване на изображението на лицето на даден човек (снимка или видео), наречено биометрична „**проба**“, е възможно да се извлече цифрово представяне на отличителните характеристики на това лице (това се нарича „**образец**“)[23]. В допълнение, Комитетът припомня, че „[б]иометричният образец е цифрово представяне на уникалните характеристики, извлечени от биометрична проба, и може да се съхранява в биометрична база данни“[24], което позволява уникалното идентифициране на дадено физическо лице. Освен това „[т]ози образец би трябвало да е уникален и специфичен за всеки човек и по принцип е постоянен“[25]. Обикновено при процеса на сравнение, с който се цели идентифицирането или проверката на самоличността на даден човек чрез лицево разпознаване, входящият

[20] Което означава, че понастоящем или изобщо не се извършва проверка, или се проверява единствено наличието на бордна карта. Например въз основа на Протокола от 22 май 1954 г. относно освобождаването на гражданите на Дания, Норвегия, Финландия и Швеция от задължението да разполагат с паспорт или разрешение за пребиваване, докато пребиват в скандинавска държава, различна от собствената им държава, считано от 1 юли 1954 г. гражданите на Дания, Норвегия, Финландия и Швеция са освободени от задължението да разполагат с паспорт или друг средство за установяване на самоличността по време на пътуване, когато пътуват между тези държави.

[21] Вж. също съображения 51, 52 и 53 от ОРЗД.

[22] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 74.

[23] Насоки № 05/2022 на ЕКЗД относно използването на технология за лицево разпознаване в областта на правоприлагането, версия 2.0, приети на 26 април 2023 г. (наричани по-нататък „**Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането**“), точки 7 и 8.

[24] Пак там, точка 9.

[25] Пак там.

биометричен образец се сравнява със съхраняваните обекти, така че да се провери дали е налице съвпадение или да се намери съвпадение в база данни[26].

21. Технологиите за лицево разпознаване могат да изпълняват две отделни функции — установяване на автентичността[27] и идентифициране[28]. Въпреки че двете функции са различни, и двете са свързани с обработването на биометрични данни, свързани с идентифицирано или подлежащо на идентифициране физическо лице[29], и следователно представляват обработване на специални категории лични данни съгласно член 9 от ОРЗД[30].

22. По-специално:

> **Установяването на автентичността** е насочено към потвърждаването на биометрично твърдение чрез сравнение. Това се нарича също „проверка 1 към 1“.
>
> **Идентифицирането** е насочено към търсене в база данни за биометрична регистрация с цел да се установят идентификатори, свързани с конкретно физическо лице. Това се нарича още „идентифициране 1 към много“.

23. И в двата случая (т.е. идентифициране и проверка на самоличността) техниките за лицево разпознаване се основават на очаквано съвпадение между образците, т.е. сравнявания образец и базовата линия(и). От тази гледна точка случаите са вероятностни: при сравнението се прави извод за по-голяма или по-малка вероятност лицето действително да е това, чиято автентичност трябва да бъде удостоверена или което трябва да бъде идентифицирано; ако тази вероятност надвишава определен праг в системата, определен от потребителя или разработчика на

---

[26] Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точки 10—11; вж. също международен стандарт ISO/IEC 2382-37, 2022-03, на разположение на адрес: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [последно осъществен достъп на 23 май 2024 г.] (наричан по-нататък „**ISO/IEC 2382-37**“)

[27] Комитетът отбелязва, че в член 3, точка 36 от предстоящия Регламент на Европейския парламент и на Съвета за установяване на хармонизирани правила относно изкуствения интелект (Акт за изкуствения интелект) (все още непубликуван в Официален вестник) „биометрична проверка“ се определя като „автоматизирана проверка „едно към едно“, включително удостоверяване, на самоличността на физически лица чрез съпоставяне на техните биометрични данни с предварително предоставени биометрични данни“ (вж. законодателна резолюция на Европейския парламент от 13 март 2024 г. относно предложението за регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на Съюза (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Пак там, в член 3, точка 35 от Акта за изкуствения интелект „биометрична идентификация“ се определя като „автоматизирано разпознаване на физически, физиологични, поведенчески и психологически човешки характеристики с цел установяване на самоличността на дадено физическо лице чрез съпоставяне на биометрични данни на това лице с биометрични данни на лица, съхранявани в база данни“.

[29] ISO/IEC 2382-37.

[30] Член 4, точка 14 от ОРЗД и Насоки 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точка 12.

системата, системата ще приеме, че е налице съвпадение от гледна точка на идентифицирането или установяването на автентичността[31].

[31] Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точка 11. Вж. също ISO/IEC 2382-37.

3 ПО СЪЩЕСТВОТО НА ИСКАНЕТО

3.1 Общи бележки

24. В настоящия раздел се анализират въпросите, представени в точка 4 по-горе. В тази връзка по отношение на въпрос 1 Комитетът ще анализира съвместимостта с член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД, а по отношение на въпрос 2 ще анализира съвместимостта с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД.

25. За тази цел Комитетът ще анализира четири различни сценария[32], чиито специфични характеристики са описани по-долу в раздел 3.2.

26. Като предварителна забележка Комитетът припомня, че използването на биометрични данни, и по-специално на технологии за лицево разпознаване, води до повишени рискове за правата и свободите на субектите на данни. На първо място, разглежданото обработване се отнася до биометрични данни, които се ползват от специална защита съгласно член 9 от ОРЗД. По-специално биометричните данни променят необратимо отношението между тялото и самоличността, защото правят характеристиките на човешкото тяло машинно разпознаваеми и подлежащи на по-нататъшна употреба[33]. Освен това използването на технологии за лицево разпознаване може да породи рискове, свързани с фалшиви отрицателни резултати, пристрастност и дискриминация[34], а потенциалната злоупотреба с биометрични данни би могла да окаже сериозни последици за физическите лица, като например измама със самоличността или измама на основата на прилика[35]. Следва също така да се отбележи, че когато лицевото разпознаване се извършва дистанционно и без активното участие на субекта на данни, хората може да са дори още по-слабо осведомени за това обработване и свързаните с него рискове. На последно място е важно да се подчертае, че характеристиките, на които са основани

[32] Четирите сценария, анализирани от Съвета, са основани на случаите на употреба, представени в приложение I към искането. Френският НО поясни, че случаите на употреба, представени в приложение I към искането, представляват примери за прилагане, спадащи към даден сценарий, които се използват с илюстративна цел.

[33] Становище 3/2012 на Работната група по член 29 относно развитието на биометричните технологии, прието на 27 април 2012 г., WP193 (наричано по-нататък „**Становище 3/2012 на РГ 29 относно биометричните технологии**“), стр. 4. Следва да се отбележи, че в настоящото становище се прави препратка към Директива 95/46/ЕО от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни („Директивата за защита на данните“). С ОРЗД бе разширен обхватът на специалните категории данни, като за разлика от Директивата за защита на данните в ОРЗД се предвижда, че биометричните данни представляват специални категории данни (член 9 от ОРЗД).

[34] Насоки относно лицевото разпознаване, Консултативен комитет на Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни, юни 2021 г., стр. 15; също така Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точка 27.

[35] Становище 3/2012 на РГ 29 относно биометричните технологии, стр. 29.

биометричните данни, като цяло могат да се считат за постоянни и следва да се третират като неотменими, особено в рамките на лицевото разпознаване[36].

27. Поради това, като се взема предвид горепосоченото, преди да прибягнат към използването на такива технологии, дори ако те следва да се считат за особено ефективни, администраторите следва да оценят въздействието върху основните права и свободи на субектите на данни и да преценят дали законната цел на обработването може да се постигне със средства, които представляват по-малка намеса[37].

28. Комитетът също така припомня, че правото на защита на личните данни не е абсолютно право, а следва да бъде в равновесие с другите основни права, защитени с Хартата, съгласно принципа на пропорционалност[38].

29. В член 25, параграф 1 от ОРЗД се посочват „принципите за защита на данните“, изброени в член 5 от ОРЗД[39], и се изисква „ефективното прилагане“ на тези принципи на етапа на проектирането[40]. Това изрично включва принципа за свеждане на данните до минимум по член 5, параграф 1, буква в) от ОРЗД[41], съгласно който личните данни трябва да бъдат „подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се

[36] Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точка 104.

[37] Съображение 39 от ОРЗД. Вж. също Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 73.

[38] Съображение 4 от ОРЗД. В това отношение вж. също решение на Съда от 22 юни 2021 г., *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (наричано по-нататък „дело C-439/19 *Latvijas Republikas Saeima*“), точки 98, 110 и 113. Освен това принципът на пропорционалност, като общ принцип на правото на Съюза, изисква установените с акт на Съюза мерки да бъдат в състояние да осъществят легитимните цели, преследвани от съответната правна уредба, и да не надхвърлят необходимото за тяхното постигане (вж. решение на Съда от 9 ноември 2010 г., *Volker und Markus Schecke u Eifert*, C-92/09 и C-93/09, ECLI:EU:C:2010:662 (наричани по-нататък „дела C-92/09 и C-93/09 *Volker und Schecke*“), точка 74 и цитираната съдебна практика).

[39] Насоки № 4/2019 на ЕКЗД относно член 25, Защита на данните на етапа на проектирането и по подразбиране, версия 2.0, приети на 20 октомври 2020 г. (наричани по-нататък „**Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране**“), точка 11.

[40] Член 25, параграф 1 от ОРЗД гласи: „Като взема предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, например псевдонимизация, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване, за да се спазят изискванията на настоящия регламент и да се осигури защита на правата на субектите на данни“. Вж. също Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, точка 13.

[41] В съответствие с това в съображение 39 от ОРЗД се посочва, че личните данни следва да се обработват единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства.

обработват, и който дава израз на посочения принцип на пропорционалност“[42]. Освен това в член 25, параграф 2 от ОРЗД се уточнява задължението за „свеждане на данните до минимум по подразбиране“, като се посочва, че то се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност[43].

30. Член 25 от ОРЗД обаче не изисква осъществяването на специфични технически или организационни мерки от страна на администраторите, а вместо това изисква избраните мерки и гаранции да бъдат подходящи с оглед на контекста и на породените от обработването рискове за правата и свободите на субекта на данни[44]. По подобен начин член 32 от ОРЗД относно сигурността на обработването изисква администраторите и обработващите лични данни да прилагат подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с риска за правата и свободите на физическите лица.

31. Важно е да се отбележи, че дори пътниците да дадат изричното си съгласие за използването на биометричните им данни с цел да се рационализира пътникопотока на летищата, свързаните с обработването принципи на необходимост и пропорционалност, залегнали в ОРЗД, продължават да се прилагат и трябва да се спазват[45].

32. По отношение на **принципа на необходимост** Комитетът ще проучи дали предложеното обработване е необходимо, за да се постигне преследваната цел и дали същата цел може да се постигне по толкова ефикасен начин с други средства, които засягат в по-малка степен основните права на субектите на данни[46]. По отношение на **принципа на пропорционалност** Комитетът ще прецени дали отрицателното въздействие върху основните права и свободи на субектите на данни е пропорционално на очакваните ползи. Ако ползите са относително малки, въздействието може да не е пропорционално[47].

33. Във всеки случай, дори Комитетът да счете, че един от сценариите, анализирани по-долу, би могъл да отговаря на изискванията на член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД, администраторът трябва да докаже това с помощта на фактически елементи във всеки отделен случай. Това доказване следва да включва обмислянето на алтернативни сценарии.

---

[42] Дело C-439/19 *Latvijas Republikas Saeima*, точка 98; решение на Съда от 11 декември 2019 г., *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (наричано по-нататък „дело C-708/18 *M5A-ScaraA*“), точка 48.

[43] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, точка 48.

[44] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, точка 14.

[45] Насоки 5/2020 на ЕКЗД относно съгласието в съответствие с Регламент 2016/679, точка 5.

[46] Дело C-439/19 *Latvijas Republikas Saeima*, точки 110 и 113; решение на Съда (голям състав) от 4 юни 2023 г., *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, точка 108.

[47] Дело C-708/18 *M5A-ScaraA*, точки 52—56, дела C-92/09 и C-93/09 *Volker und Schecke*, точка 87, дело C-439/19 *Latvijas Republikas Saeima*, точки 98, 110, 113. Вж. също Становище 3/2012 на РГ 29 относно биометричните технологии, стр. 8.

3.2 По съвместимостта с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД

3.2.1 Сценарий 1: съхраняване на регистриран биометричен образец единствено от физическото лице, с цел проверка на самоличността

34. В настоящия раздел се разглежда съвместимостта с член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД на съхраняването на биометричния образец на пътника единствено от физическото лице, например в индивидуалното му устройство[48], под негов изключителен контрол[49], с цел проверка на самоличността[50] (наричан по-нататък „**сценарий 1**“). В настоящия раздел също така се разглеждат подходящите гаранции за сценарий 1 с оглед на членове 25 и 32 от ОРЗД.

Описание на сценария

35. В сценарий 1 регистрираният биометричен образец на всеки пътник, който е дал своето съгласие за такова обработване, се съхранява единствено от него, например в индивидуално устройство, притежавано от него, и под негов изключителен контрол. Самоличността на пътниците се удостоверява (сравнение 1:1) при преминаването им през конкретни пунктове за проверка на летището.

36. Регистрацията се извършва от летищния оператор, било то дистанционно чрез приложението на летищния оператор[51], или на терминалите на летището с подходящо ниво на достоверност по отношение на самоличността (например подходящо ниво на достоверност съгласно eIDAS[52]). Тази регистрация се състои в записването в устройството на пътника на необходимите за обработването биометричен образец и данни за идентификация[53] (наричани по-нататък „**идентификационни данни**“). Регистрацията се извършва само веднъж и е с конкретен период на валидност (например съвпадащ с периода на валидност на паспорта на пътника). След процеса по регистрация летищният оператор не запазва нито идентификационните, нито биометричните данни на пътниците.

37. Що се отнася, по-специално, до съхранението, идентификационните данни и биометричният образец на пътника се съхраняват на място в устройството на всеки пътник (например в мобилното приложение на летищния оператор или в приложение за цифров портфейл). Впоследствие устройството може да се използва за предаване на идентификационните данни и биометричните образци на пътниците или за получаване на достъп до тях, като евентуално се включва информация за полета и/или бордната карта. Например тази информация е

[48] Като алтернатива лицето би могло да отпечата и да съхранява биометричния си образец на хартиен носител.
[49] Това не засяга общата отговорност на администратора във връзка с обработването.
[50] Както е онагледен от случай на употреба 1 в приложение I към искането.
[51] ЕКЗД отбелязва, че в бъдеще биха могли да се предвидят алтернативни начини за тази регистрация, като тя евентуално ще може да се извършва без специфично приложение на летищния оператор — например посредством взаимодействие с цифровия портфейл на потребителя.
[52] Рамка за електронната идентификация и удостоверителните услуги (наричана по-нататък „**eIDAS**“), основана на Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност.
[53] За целите на настоящото становище „идентификационни данни“ означава данни като фамилно име, собствено име, дата на раждане и др., чиято точност е проверена в документ за самоличност или паспорт.

криптирана с ключ, достъпен единствено за летищния оператор, евентуално под формата на код за бърза реакция, който може да бъде отпечатан на хартиен носител или показан на екрана на устройството на пътника. В този случай пътникът ще покаже този код за бърза реакция на специалните контролни устройства на летището, оборудвани с камера и скенер на кодове за бърза реакция.

38. От гледна точка на сигурността, по време на съпоставянето кодовете за бърза реакция се декриптират с помощта на ключ, достъпен за летищния оператор, като единствено той може да декриптира кодовете за бърза реакция. Биометричните данни на пътниците се запазват само за много кратък период от време и се заличават след приключване на съпоставянето. Следва да се отбележи, че мерките за сигурност по отношение на съхраняването зависят отчасти от сигурността на устройството на пътника.

Оценка на ЕКЗД

39. В сценарий 1 са описани техническите и организационните мерки, предвидени с цел да се осигури ниво на сигурност, съобразено с рисковете за субектите на данни, както се изисква съгласно член 5, параграф 1, буква е) и член 32 от ОРЗД. Самоличността на пътниците се удостоверява (сравнение 1:1) при преминаването им през конкретни пунктове за проверка на летището. В този сценарий основната операция по съпоставяне се извършва в условията на контролирана среда[54], като пътниците участват активно и разполагат с повече контрол върху своите данни. По-конкретно, проверяват се единствено пътниците, които са дали съгласие за такова обработване, и тъй като проверката се извършва на места със специализирани устройства, не се събират биометрични данни на останалите пътници, които не са дали съгласие за такова обработване. Освен това пътниците, които са дали своето съгласие, могат да спрат обработването във всеки един момент, като заличат данните от своите устройства.

40. Използването на лицево разпознаване, основано на биометричен образец, който се съхранява единствено от физическото лице, например в притежавано от пътника индивидуално устройство под негов изключителен контрол, и който се използва за удостоверяване на самоличността в конкретни пунктове за проверка посредством специален интерфейс, при определени условия поражда по-малко рискове в сравнение с използването на биометрични данни, при което данните се съхраняват в централизирана база данни[55]. Когато такова съхраняване на място е придружено от подходящи гаранции[56], сериозността на нарушенията на сигурността на личните данни се намалява в сравнение с централизираното съхраняване от

[54] „Неконтролирана среда“ означава използването на лицево разпознаване за установяване на самоличността без активното участие на субектите на данни, при което образецът на всяко лице, влизащо в зоната за наблюдение, се сравнява с образци от широка извадка от населението, съхранявани в база данни, вж. Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точка 17.
[55] Насоки № 5/2022 на ЕКЗД относно лицевото разпознаване в правоприлагането, точка 17.
[56] Както е разгледано по-долу в точка 46.

гледна точка на броя на засегнатите лица и се гарантира, че достъпът до биометричния образец включва активното участие на субекта на данни.

41. Освен това съпоставянето би могло да се извършва на място, на летището, например чрез сравняване на биометричния образец, съдържащ се в кода за бърза реакция, с резултата от изчисляването на образеца въз основа на биометричната проба, заснета от камерата на контролното устройство. Администраторът, който извършва конкретна проверка (като това може да бъде или летищен оператор, или авиокомпания в зависимост от това дали проверката се извършва на пунктовете за проверка за сигурност на летищата, при оставянето на багажа, отвеждането към самолета и/или при влизането в салоните за пътници), узнава и използва единствено резултата от съпоставянето. Освен това фактът, че информацията, необходима за съпоставянето (например кода за бърза реакция), трябва да бъде предоставена от лицето, действа като втори фактор[57] и по този начин подсилва сигурността на удостоверяването на автентичността.

42. Що се отнася до съвместимостта с член 25 от ОРЗД, и по-специално с цел да се спази изискването за свеждане на данните до минимум, следва да се гарантира, че обработването отговаря на принципа на необходимост. В сценарий 1 би могло да се счете, че избраните мерки отговарят на принципа на необходимост във връзка с преследваната цел (а именно рационализиране на пътникопотока), ако в зависимост от обстоятелствата, при които се извършва обработването, администраторът може да докаже, че няма алтернативни решения, които представляват по-малка намеса и които биха могли да постигнат същата цел със същата ефективност. Администраторът може например да е в състояние да докаже, че дори ако се налага пътниците да показват своите устройства, сценарий 1 ускорява процеса на проверка в сравнение с настоящото положение, включващо проверка от човек дали името на бордната карта отговаря на документа за самоличност на пътника[58]. Следва да се отбележи, че това не би могло да се докаже, ако понастоящем не се извършват проверки за удостоверяване на самоличността на пътниците въз основа на официалните им документи за самоличност (в това отношение вж. точка 18 по-горе).

43. Освен това биометричните образци не се запазват от летищния оператор след регистрацията, а периодът на съхранение на биометричните данни от администратора, извършващ проверката, е изключително кратък, тъй като тези данни се заличават непосредствено след приключване на съпоставянето. По този начин избраните в сценарий 1 мерки изглежда ограничават степента на обработването и срока на съхранение на личните данни.

44. Що се отнася до принципа на пропорционалност, намесата в резултат на такова обработване може да бъде неутрализирана от активното участие на пътниците, тъй като биометричните им данни се съхраняват само от тях. Освен това, като се вземат предвид описаните по-горе мерки и като се приема, че администраторът прилага подходящи гаранции, необходими за конкретното обработване, прилагането на подходящи мерки би могло да осигури ниво на сигурност, което съответства на риска. В този случай отрицателното въздействие върху

[57] Например по този начин се ограничава рискът от фалшифициране на самоличността. Вж. също гаранция B.1.2 по-долу.

[58] Би могло да се твърди, че при проверката на биометричните данни е възможно да има по-малка вероятност от грешки в сравнение с проверката от човек.

основните права и свободи на субектите на данни би могло да се счита за пропорционално на очакваните ползи.

45. Поради това, като се взема предвид горепосоченото, в отговор на въпрос 1.1 Комитетът заключава, че това обработване **принципно би могло да се счита за съвместимо с член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД при наличие на подходящи гаранции**.

Подходящи гаранции

46. В отговор на въпрос 1.2, в този вид сценарий ЕКЗД счита, че следва да бъдат приложени най-малко следните гаранции. Биха могли да се използват и други гаранции, различни от описаните в настоящото становище, за постигането на същите цели във връзка със сигурността и защитата на данните, като те биха могли да са законни, при условие че осигуряват спазването на приложимата правна уредба.

47. Забележка: това е неизчерпателен преглед на високо равнище на възможните подходящи гаранции, които следва да се приложат от администратор в решение, подобно на сценарий 1. За преценката дали са подходящи съгласно членове 25 и 32 от ОРЗД е необходим анализ на всеки отделен случай. Всички администратори ще трябва да гарантират, че извършват своя собствена оценка на въздействието върху защитата на данните (наричана по-нататък „ОВЗД“)[59], като е възможно за конкретните им решения да са необходими допълнителни мерки, които не са включени в настоящото становище.

А. Общи аспекти

А.1 Оценка на въздействието върху защитата на данните

А.1.1 Извършване на ОВЗД в съответствие с изискванията на член 35 от ОРЗД във всеки случай, в който администраторът планира нова операция по обработване, включваща обработване, което има вероятност да породи висок риск. Сценарий 1 вероятно представлява такъв случай, тъй като той включва широкомащабно обработване на биометрични данни[60]. Оценка дали е подходящо да се внедри система за лицево разпознаване, включително необходимостта от такава система и нейната пропорционалност по отношение на преследваните цели[61], по време на ранния етап на проектиране, както и преглед на системата през целия жизнен цикъл на разработването на продукта;

[59] Член 35 от ОРЗД.
[60] Член 35, параграф 3 от ОРЗД и насоките на РГ 29 относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, приети на 13 октомври 2017 г., РД 248 ред. 01, одобрени от ЕКЗД.
[61] Член 35, параграф 7, буква б) от ОРЗД.

А.1.2 Консултиране със съответния надзорен орган, ако обработването все пак поражда висок риск въпреки предприетите от администратора мерки за ограничаване на риска[62].

А.2 Права на субектите на данни и гаранции, които могат да се приложат от администраторите

А.2.1 Гаранции за справяне със случаи на фалшиви отрицателни резултати. Ограничаване на риска от пристрастност въз основа на възраст, пол и раса, като „редовно трябва да се оценява дали алгоритмите функционират съобразно приложимите цели и те да се коригират с цел смекчаване на установените отклонения, и да се обезпечи добросъвестността на обработването“[63]. Например чрез осъществяване на човешки надзор и намеса, за да се смекчат евентуалните отклонения и да се гарантира, че пътниците не стават обект на дискриминация или профилиране;

А.2.2 Гарантиране, че цялото обработване на лични данни е прозрачно и че хората са осведомени и контролират начина, по който данните им се обработват, за всяка операция по обработване[64];

А.2.3 Гарантиране, че са въведени мерки за спазване на принципа на ограничаване в рамките на целта, така че данните да не се използват за други цели, например за такива, свързани със сигурността, или за обучение;

А.2.4 Гарантиране, че не се заснемат фотографски изображения или видеоклипове, дори да не се записват и да не се обработват, на лица, които не са дали съгласие за лицево разпознаване, посредством подходящи мерки (като например използване на подходяща дълбочина на полето и зона на заснемане, за да се избегне заснемането на изображения на други пътници, намиращи се в близост или на заден план, обособяване на специални и ясно обозначени опашки за лицево разпознаване);

А.2.5 Изчакване на утвърдително действие от даващ съгласието си пътник, преди да се премине към заснемането на фотографски изображения или видеоклипове, когато едни и същи устройства може да се използват от пътници, дали съгласие за лицево разпознаване, и от пътници, които не са дали съгласие за това, или когато е възможно

[62] Член 36, параграф 1 от ОРЗД.
[63] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, бележка под линия 60, точка 70.
[64] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, точка 68 и съображение 7 от ОРЗД.

пътници, които не са дали съгласие за лицево разпознаване, да попадат във визуалния обсег на системата, докато тя не се използва;

А.2.6 Възможност субектът на данни във всеки един момент да извърши заличаване на данни, достъпни единствено за него (биометричен образец[65]), които се съхраняват в мобилно приложение или цифров портфейл[66];

А.2.7 Наличие на жизнеспособни алтернативи или на резервни решения (т.е. за пътници, които не дават съгласие за използване на биометричните им данни, за пътници, които не могат да използват такива решения, или за пътници, получили грешен отказ), така че да се гарантира също, че пътниците, които не дават съгласие, не търпят неудобства[67];

А.2.8 Ако се използва приложение, то следва да подлежи на внимателно проектиране и конфигуриране, за да не се събират ненужни данни и да се избягва използването на комплекти за разработване на софтуер (КРС) на трети страни, които събират данни за други цели.

А.3 Отчетност

А.3.1 Проучване дали съществуват приложими кодекси за поведение или механизми за сертифициране, които да спомогнат да се докаже съответствието със сигурността на обработването съгласно член 32 от ОРЗД[68]. Проверка дали мерките са подходящи за конкретното обработване, което се предвижда. Стандартите[69], най-добрите практики и кодексите за поведение, признати от сдружения и други органи, представляващи съответните категории администратори, могат да бъдат от полза при определянето на подходящите мерки;

А.3.2 Гарантиране, че на устройствата на ползвателите се правят основни проверки за сигурност, за да се позволи провеждането на етапа на регистрация, въпреки че пътникът също изпълнява определена роля по отношение на защитата на своите данни, тъй като те се съхраняват в неговото устройство. В раздел В.2 „Инфраструктура и мрежа“ по-долу са представени примери за такива технически проверки и контрол.

[65] Препратките към биометричен образец в гаранциите за сценарий 1 съответстват на препратките към ключ/тайна в сценарий 2.
[66] Следва да се има предвид, че тази гаранция се прилага само за сценарий 1.
[67] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 86.
[68] Член 32, параграф 3 от ОРЗД и Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, точка 10.
[69] Вж. например ISO/IEC 2382-37.

Б. Организационни аспекти:

Б.1 Политика и съответствие

Б.1.1. Гарантиране, че е въведен вътрешен контрол на достъпа[70] с правила за администраторите;

Б.1.2 Когато услугата за лицево разпознаване може да се предоставя от една от страните, участващи в обработването, без да се налага останалите участващи страни да си служат с идентификационните или биометричните данни, или и с двата вида данни — забрана тези данни да преминават през въпросните други страни. Например не е необходимо авиокомпанията да осъществява технически достъп до биометричните данни, когато използва общата летищна инфраструктура, дори когато авиокомпанията действа като администратор на обработването съгласно ОРЗД;

Б.1.3 Определяне на политика за криптиране и управление на ключовете[71], например за обработване на идентификационни и биометрични данни;

Б.1.4 Гарантиране на съответствие с глава V от ОРЗД. Например следва да се гарантира предаване, което отговаря на изискванията, ако по време на процеса по регистрация администраторът използва дистанционна услуга, установена в трета държава;

Б.1.5 Гарантиране, че е сключено споразумение с обработващ лични данни[72] в съответствие с член 28, параграф 3 от ОРЗД, когато се използват услугите на обработващи лични данни;

Б.1.6 Гарантиране, че се въвеждат процедури за управление на човешкия надзор и намесите, по-специално за справяне със случаи на фалшив отказ, както и при проблеми, свързани с техническите характеристики и използването на системата.

Б.2 Обучение и изпитване

Б.2.1 Гарантиране, че персоналът е обучен по подходящ начин;

---

[70] Насоки № 4/2020 на ЕКЗД относно използването на данни за местонахождение и инструменти за проследяване на контакти във връзка с пандемията от COVID-19, приети на 21 април 2020 г. (наричани по-нататък „**Насоки № 4/2020 на ЕКЗД относно данните за местонахождение и инструментите за проследяване на контакти**“), SEC-10, стр. 16.

[71] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 89.

[72] Член 28, параграф 3 от ОРЗД.

Б.2.2 Внедряване на „процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването“[73];

Б.2.3. Внедряване на процес, с който се гарантира, че обработването на биометричния образец на пътника[74] с цел удостоверяване на автентичността се извършва по технически ефективен начин и е достатъчно точно;

Б.2.4. Гарантиране, че биометричните проби, които се събират при регистрацията и на пункта за проверка, са с достатъчно добро качество за извършването на надеждно обработване на биометрични данни.

В. Технически аспекти:

В.1 Достъп

В.1.1 Прилагане на гаранции по време на етапа на регистрация, за да се гарантира процес на регистрация по метода bootstrap с проверена самоличност. Например за подсилване на оценката на многофакторното удостоверяване на самоличността на ползвателя могат да се предприемат стъпки, вариращи от защитени с парола еднократни връзки за активиране на приложението до механизми на място за разблокиране на устройството;

В.1.2 Прилагане на гаранции за справяне със случаи на фалшиви положителни резултати и с действия, насочени към фалшифициране на самоличността, както и за предотвратяване на измами[75];

В.1.3 Забрана на всякакъв външен достъп до идентификационните и биометричните данни[76];

В.1.4 Гарантиране, че обработването се извършва на място на етапите на регистрация, предаване и съпоставяне. Точката, в която се извършва съпоставянето, следва да е разположена възможно най-близо до устройството на лицето. Разрешаването на съпоставяне с образеца в устройството на лицето може да налага взаимодействие с доставчици на услуги, разположени извън летището, и да включва използването на ресурсите на обществена мрежа, в резултат на което се засяга достъпността, а образецът се разпространява сред външни субекти;

[73] Член 32, параграф 1, буква г) от ОРЗД.
[74] Препратките към биометричен образец в гаранциите за сценарий 1 съответстват на препратките към ключ/тайна в сценарий 2.
[75] Доклад на АЕСКС относно цифровата самоличност: използване на понятието за самоличност под контрола на самото лице (SSI) за изграждане на доверие, януари 2022 г.
[76] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 89.

B.1.5 Проверка на самоличността на ползвател за добавяне на нов полет и генериране на нов криптиран код за бърза реакция;

B.1.6 Предприемане на мерки за справяне със ситуация, в която пътникът може да загуби достъпа до своя код за бърза реакция.

B.2 Инфраструктура и мрежа

B.2.1 Обвързване с условия операционната система (ОС) да се поддържа в актуален вид и проверяването на самоличността да е позволено с цел осъществяване на достъп до устройството, за да работи приложението/цифровият портфейл, включително с автоматично заличаване на идентификационните и биометричните данни, ако ОС не е актуална и поражда рискове за сигурността;

B.2.2 Изолиране на извършващите съпоставяне единици (т.е. летищните устройства) от мрежата, докато са в работен режим, и предприемане на всички други необходими мерки, за да се гарантира сигурността;

B.2.3 Извършване на биометрично съпоставяне в устройството на пътника или в летищното устройство (периферни изчисления);

B.2.4 Решения за преодоляване на свързани със сигурността уязвимости на индивидуалните устройства на пътниците, включително криптиране (като минимум) на биометричните и идентификационните данни, когато не се използват;

B.2.5 Използване на сигурно съхранение (най-малко) на биометричните данни, достъпни единствено за ползвателя[77], например чрез използване на т. нар. „сигурен анклав“ на смартфон;

B.2.6 Мерки за защита, които целят осигуряване на физическата сигурност на помещенията, включително на биометричния терминал на летището. Осигуряване на високо ниво на сигурност за елементите от архитектурата, които обработват идентификационни и биометрични данни (например изчисление, информационен поток, временно или дългосрочно съхраняване).

B.3 Сигурност и управление на данните за проверка за установяване на самоличността на ползвателя

[77] Препратките към биометричен образец в гаранциите за сценарий 1 съответстват на препратките към ключ/тайна в сценарий 2.

B.3.1 Сегментиране на данните при тяхното предаване и съхранение на най-малко три различни групи, като: идентификационни данни, биометрични данни и информация за полета[78]. Гарантиране, че данните са криптирани по подходящ начин между предаването и съхранението;

B.3.2 Внедряване на технически мерки за гарантиране, че в конкретен пункт за проверка се обработват и проверяват единствено данните, които могат да се обработват законно в този пункт;

B.3.3 Гарантиране на ефективността на заличаването на данни[79] чрез сигурна процедура за заличаване (например основна памет, свръхоперативна памет, евентуални резервни копия) и преценка кога заличаването на данните следва да бъде автоматизирано. Периодите на съхранение на данните следва да се съблюдават строго чрез автоматични рутинни действия, без да е необходимо допълнително действие от страна на лицето[80];

B.3.4 Гарантиране на автентичността и цялостността на данните (например на подпис)[81];

B.3.5 Запазване на биометричните данни на пътниците в пункта за регистрация и за проверка само за много кратък период и заличаването им непосредствено след като пътникът премине през пункта за проверка;

B.3.6 Ако за регистрацията се използва приложение, прилагане на стандарти за сигурност във връзка със сигурността на мобилното приложение по време на разработването на приложението, както и изпитвания за сигурност от трета страна;

B.3.7 Гарантиране, че са въведени мерки за сигурност по време на етапа на регистрация на летището, за да се запази поверителността и цялостността на биометричните данни на пътника. Например, ако гишето отпечатва кода за бърза реакция, той не следва да се показва на гишето, за да се избегне заснемането му от злонамерено лице. При предаване на къси разстояния предаването следва да се извършва с активното участие на ползвателя, като се използва канал, който гарантира близост;

B.3.8 Данните, достъпни единствено за физическото лице[82], следва да се държат в място за сигурно съхранение в устройството на лицето, а по отношение на всички възможни

[78] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 89.
[79] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 89.
[80] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране съгласно член 25, точка 82.
[81] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 89.
[82] Препратките към биометричен образец в гаранциите за сценарий 1 съответстват на препратките към ключ/тайна в сценарий 2.

уязвимости, свързани с операционната система на устройството, трябва да бъдат приложени подходящите софтуерни поправки за защита. В случай на отпечатан код за бърза реакция лицето следва да бъде осведомено за особено чувствителното естество на данните, които съдържа кодът, и какви действия позволява да бъдат извършени;

B.3.9 Гарантиране, че регистрацията се извършва при съблюдаване на адекватни техники за доказване на самоличността от разстояние[83].

3.2.2 Сценарий 2: централизирано съхраняване на регистриран биометричен образец в рамките на летището в криптирана форма с ключ/тайна, достъпни единствено за пътника, с цел проверка на самоличността

48. В настоящия раздел се разглежда съвместимостта с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД на централизираното съхраняване — с цел проверка на самоличността— на регистрирани биометрични образци на пътниците в централизирана база данни, в криптирана форма и с ключ/тайна, достъпни единствено за пътника[84] (наричан по-нататък „**сценарий 2**“). В настоящия раздел също така се разглеждат подходящите гаранции за сценарий 2 с оглед на членове 25 и 32 от ОРЗД.

Описание на сценария

49. В сценарий 2 регистрацията се извършва само веднъж за определен период на валидност (с продължителност например от една година след последния полет до изтичането на валидността на паспорта), било то дистанционно при подходящо ниво на достоверност по отношение на самоличността (например, подходящо ниво на достоверност съгласно eIDAS) или на терминалите на летището. Регистрацията се контролира от летищния оператор и се състои от генериране на идентификационни и биометрични данни, които се криптират с ключ/тайна.

50. Базата данни се съхранява в помещенията на летището, като е под контрола на летищния оператор. Криптографските ключове/тайни, отнасящи се до конкретно лице, се съхраняват единствено в устройството на лицето (например в мобилното приложение на летищния оператор). Приложението може да генерира код за бърза реакция, съдържащ ключа/тайната, като те може да бъдат отпечатани на хартиен носител или показани на екрана на устройството[85]. В допълнение, летищният оператор осигурява второ ниво на криптиране[86], като ключовете са под негов контрол.

---

[83] Вж. доклада на АЕСКС относно доказването на самоличността от разстояние: анализ на методите за извършване на действия за доказване на самоличността от разстояние, март 2021 г.

[84] Както е онагледено от случай на употреба 2 в приложение I към искането.

[85] Френският НО допълнително поясни, че може да има и други технически решения за изпращане на необходимата информация, като например използване на протокол за комуникация на къси разстояния.

[86] Самият ключ/тайна (достъпни за лицето) са криптирани с друг ключ, който се държи от летищния оператор.

51. Автентичността на пътниците се удостоверява (сравнение 1:1) при преминаването им през конкретни пунктове за проверка на летището. Пътниците, които избират да преминат през пунктовете за проверка на биометрични данни, показват своя код на специалното контролно устройство, оборудвано с камера и скенер на кодове за бърза реакция. Индексът на пътника се изпраща до базата данни с искане за криптирания образец, който се изтегля и проверява на място в летищното устройство и/или в устройството на ползвателя. Администраторът на пункта за проверка узнава и използва единствено резултата от съпоставянето[87].

52. В този сценарий между летищата не е налице обмен на идентификационни и биометрични данни, като централните бази данни не са нито взаимосвързани, нито оперативно съвместими.

Оценка на ЕКЗД

53. В сценарий 2 регистрираните биометрични образци на пътниците се съхраняват централизирано, но в криптирана форма, с ключ/тайна, достъпни единствено за пътника. В сценарий 2 автентичността на пътниците се удостоверява (сравнение 1:1).

54. Хипотезата в този сценарий е, че целта за рационализиране на пътникопотока (т.е. чрез увеличаване на бързината на проверките) би могла да се постигне с помощта на централизирана система. В предходни случаи ЕКЗД отбеляза, че такова решение би могло да бъде счетено за работеща алтернатива на децентрализираното съхранение на регистрираните биометрични образци[88] (както е описано в сценарий 1) в случай на обективна необходимост и при наличието на подходящи гаранции (вж. гаранциите, описани в точка 60 и сл. по-долу).

55. От гледна точка на съображенията, свързани със сигурността, данните на всяко лице се криптират със специфичен ключ, достъпен единствено за лицето и под негов изключителен контрол. Освен това фактът, че информацията, необходима за съпоставянето (например тайната/ключа), трябва да бъде предоставена от лицето, действа като втори фактор[89] и по този начин подсилва сигурността на удостоверяването на автентичността. В допълнение, летищният оператор осигурява второ ниво на криптиране, като ключовете са под контрола на летищния оператор. В сценарий 2 индексът на лицето се изпраща до централната база данни, за да се извлекат биометричните данни, свързани с лицето. След това тези данни се изпращат (в криптиран вид) до компютър, разположен на пункта за проверка, където се декриптират, за да се извърши съпоставянето, като администраторът на пункта за проверка узнава и използва единствено резултата от съпоставянето. При условие че ключът/тайната на лицето се съхраняват в компютъра, разположен в пункта за проверка, и че до централната база данни се изпраща единствено индекс на пътника за извличане на криптирания биометричен образец, такива

[87] Френският НО поясни, че този период на съхранение е примерен и може да бъде счетен за приемлив с оглед на факта, че ключът се съхранява от физическото лице, а периодът може да бъде избран на етапа на регистрация. Следва обаче да се отбележи, че този период на съхранение може да бъде коригиран.
[88] Насоки 3/2019 на ЕКЗД относно видеоустройствата, точка 88.
[89] Например по този начин се ограничава рискът от фалшифициране на самоличността. Вж. също гаранция B.1.2.

мерки за сигурност биха могли да бъдат счетени за съвместими с член 5, параграф 1, буква е) и член 32 от ОРЗД.

56. Що се отнася до съвместимостта с член 25 от ОРЗД, и по-специално с цел да се спази изискването за свеждане на данните до минимум, следва да се гарантира, че обработването отговаря на принципа на необходимост. В сценарий 2 би могло да се счете, че избраните мерки отговарят на принципа на необходимост във връзка с преследваната цел (а именно рационализиране на пътникопотока на летищата), ако в зависимост от обстоятелствата, при които се извършва обработването, администраторът може да докаже, че няма алтернативни решения, които представляват по-малка намеса и които биха могли да постигнат същата цел със същата ефективност. В сценарий 2 пътниците пак ще трябва да показват своите устройства[90]. Независимо от това, администраторът може да е в състояние да докаже, че сценарий 2 ускорява процеса на проверка в сравнение с настоящото положение, включващо проверка от човек дали името на бордната карта отговаря на документа за самоличност на пътника[91], или в сравнение със сценарий 1. Следва да се отбележи, че това не би могло да се докаже, ако понастоящем не се извършват проверки за удостоверяване на самоличността на пътниците въз основа на официалните им документи за самоличност (в това отношение вж. точка 18 по-горе).

57. Що се отнася до принципа на пропорционалност, намесата в резултат на такова обработване може да бъде неутрализирана от активното участие на пътниците, които съхраняват ключа за криптираните им данни под свой изключителен контрол. Освен това изглежда, че рисковете за сигурността, произтичащи от съхраняването на биометричните данни на пътниците в централизирана база данни, ключът за които е достъпен единствено за пътниците, могат да се ограничат посредством използването на подходящи гаранции (вж. гаранциите, разгледани в точка 60 и сл. по-долу). Следователно, ако се приеме, че администраторът прилага подходящи гаранции, необходими за конкретното обработване, рисковете за лицата биха могли да се ограничат, а отрицателното въздействие върху основните права и свободи на субектите на данни биха могли да се считат за пропорционални на очакваните ползи. Естествено, във всеки случай следва да се гарантира, че се обработват единствено необходимите за целта данни и се проверяват само пътниците, дали своето съгласие, поради което няма риск от събиране на биометричните данни на останалите лица, които не са дали своето съгласие.

58. В искането се посочва като пример, че в сценарий 2 периодът на съхранение на криптираните данни в базата данни обичайно би могъл да бъде една година след последния полет, осъществен от лицето, и до изтичането на срока на валидност на паспорта. В искането не е предоставена информация за обосновка на толкова дълъг период въз основа на обективни причини, въпреки че може да се предположи, че такъв период на съхранение се предвижда с цел удобство за бъдещи полети. Що се отнася до периода на съхранение, за да се постигне съвместимост с член 5, параграф 1, буква д) от ОРЗД при този сценарий, администраторите следва да могат да обосноват защо този период на съхранение е необходим за конкретните

[90] Френският НО поясни допълнително, че е възможно да има и други варианти за представяне на образеца, например отпечатан на хартиен носител. В допълнение, ЕКЗД признава, че в бъдеще би могло да се предвиди използването на алтернативна технология, например въз основа на система за комуникация в близката зона (NFC).

[91] Би могло да се твърди, че при проверката на биометричните данни е възможно да има по-малка вероятност от грешки в сравнение с проверката от човек.

случаи. Комитетът препоръчва на администраторите да предвидят възможно най-краткия период на съхранение, като вземат под внимание и пътниците, които летят много рядко, и като предложат на субекта на данни да определи предпочитания от него период на съхранение.

59. С оглед на тези съображения, в отговор на въпрос 2.1.1 Комитетът заключава, че това обработване **принципно би могло да се счита за съвместимо с член 5, параграф 1, буква д), член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД при наличие на подходящи гаранции**.

Подходящи гаранции

60. В отговор на въпрос 2.1.2, в този вид сценарий ЕКЗД счита, че **в допълнение към гаранциите, посочени в сценарий 1**, трябва да бъдат приложени най-малко следните гаранции. Биха могли да се използват и други гаранции, различни от описаните в настоящото становище, за постигането на същите цели във връзка със сигурността и защитата на данните, като те биха могли да са законни, при условие че осигуряват спазването на приложимите правни уредби.

61. Забележка: *това е неизчерпателен преглед на високо равнище на възможните подходящи гаранции, които биха могли да се приложат от администратор в решение, подобно на сценарий 2. За преценката дали мерките са подходящи съгласно членове 25 и 32 от ОРЗД е необходим анализ на всеки отделен случай. Всички администратори ще трябва да гарантират, че извършват своя собствена ОВЗД, като е възможно за техните решения да са необходими допълнителни мерки, които не са включени в настоящото становище.*

Г. Общи аспекти

Г.1 Права на субектите на данни и гаранции, които могат да се приложат от администраторите

Г.1.1 Гарантиране, че пътникът разполага с контрол върху периодите на съхранение на всички свои данни. Периодите на съхранение трябва да бъдат ограничени до необходимото за конкретната цел. Следва да бъде определен максимален период въз основа на задълбочен анализ на фактори като срока на валидност на идентификационния документ. На субектите на данни трябва да се предложи да определят предпочитания от тях период на съхранение, който би могъл да е по-кратък от този по подразбиране;

Г.1.2 Възможност субектът на данни във всеки един момент да поиска заличаване на данни, достъпни единствено за него (ключ/тайна), които се съхраняват в мобилно приложение или цифров портфейл[92];

Г.1.3 Гарантиране, че локализацията на централната база данни позволява ефективен надзор от компетентния надзорен орган.

[92] Следва да се има предвид, че тази гаранция се прилага само за сценарий 2.

Д. Организационни аспекти:

Д.1 Политика и съответствие

Д.1.1 Доверието в централния сървър трябва да е ограничено. Гарантиране, че при управлението на централния сървър се следват ясно определени правила за управление и се прилагат всички необходими мерки за гарантиране на неговата сигурност[93].

Е. Технически аспекти:

Е.1 Достъп

Е.1.1 Поддържане на записи кой разполага с достъп до лични данни, по-специално идентификационни и биометрични данни, и кога е осъществяван достъп до тях;

Е.2 Инфраструктура и мрежа

Е.2.1 Обезопасяване по подходящ начин на централната база данни, включително срещу атаки, насочени към достъпността (availability attacks);

Е.2.2 Гарантиране, че няма интернет връзка към централната база данни, устройствата за регистрация и извършващите съпоставяне единици. Експлоатацията и поддръжката на тези системи (например създаване на резервно копие, софтуерни поправки, мониторинг и др.) трябва да се извършват на място в помещенията на летището.

Е.3 Сигурност и управление на данните

Е.3.1 Използване на най-съвременни криптографски техники, за да се осигури сигурността на обмена на данни между приложението и централизирания сървър[94];

Е.3.2 Съхраняване на индивидуалния ключ/тайна на равнището, на което ще се използва за декриптиране (т.е. в летищното устройство), и използване на индекса единствено за извличане на съответния регистриран биометричен образец в централната база данни;

---

[93] Насоки № 4/2020 на ЕКЗД относно използването на данни за местонахождение и инструменти за проследяване на контакти, PRIV-5, стр. 17.

[94] Насоки № 4/2020 на ЕКЗД относно данните за местонахождение и инструментите за проследяване на контакти, SEC-4, стр. 16: „Примерите за техники, които могат да се използват, включват: симетрично и асиметрично криптиране, хеш функции, проверка дали даден елемент се съдържа в скрит набор от данни (Private Membership Test), сравнение на скрити набори от данни (Private Set Intersection), блум филтри (Bloom filters), извличане на информация без разкриване на конкретния елемент (Private Information Retrieval), хомоморфно криптиране“.

Е.3.3 Гарантиране, че при обмена на ключа/тайната между устройството на ползвателя и летищното устройство комуникацията е защитена срещу всякакво възможно подслушване или предаване към трети страни;

Е.3.4 Индексиране на биометричния образец при съхраняването му в централната база данни, за да се позволи удостоверяване на автентичността 1:1 и да се гарантира, че той е уникален и е свързан с въпросното лице. Гарантиране, че индексът не разкрива никаква идентификационна информация на пътника и че не е свързан с криптографския ключ;

Е.3.5 Удостоверяване на автентичността и криптиране по подходящ начин на всяко предаване между централната база данни и пунктовете за проверка, като то се извършва посредством изолирани мрежи;

Е.3.6 Избягване на двупосочни връзки между набори от данни (идентификационни и биометрични данни, както и подробности за полета) и съхраняване само на уместни еднопосочни връзки в базата данни. Например да се съхраняват данни само от еднопосочни връзки от индекса към идентификационните данни, от индекса към криптираните биометрични данни и от индекса към информацията за полета;

Е.3.7 Осигуряване на мерки за непрекъснатост на дейността, например внедряване на подходящи резервни системи за съхранение;

Е.3.8 Гарантиране, че летищното устройство не съхранява записи от криптирани или некриптирани образци.

3.2.3 Централизирано съхранение на регистрираните биометрични образци с цел идентифициране

62. В настоящия раздел се разглежда съвместимостта с член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД на централизираното съхраняване — с цел идентифициране — на регистрирани биометрични образци на пътниците, когато тези образци не са криптирани с ключ/тайна, достъпни единствено за пътниците, в два случая на употреба: 1) когато тези образци се съхраняват в база данни в рамките на летището под контрола на летищния

оператор[95] (наричан по-нататък „**сценарий 3.1**“) и 2) когато тези образци се съхраняват в облака под контрола на авиокомпанията[96] (наричан по-нататък „**сценарий 3.2.**“).

63. Комитетът счита, че използването на биометрични данни с цел **идентифициране** в големи централни бази данни включва намеса в основните права на субектите на данни и евентуално би могло да породи сериозни последици за субектите на данни[97]. Освен това използването на биометрични данни следва също така да бъде разгледано във връзка с целта, за която се обработват данните, с оглед на принципите на необходимост и пропорционалност[98].

3.2.3.1 Сценарий 3.1: централизирано съхранение в база данни в рамките на летището под контрола на летищния оператор

Описание на сценария

64. В сценарий 3.1 регистрираните биометрични образци на пътниците се съхраняват в централна база данни в помещенията на летището и под контрола на летищния оператор в криптирана форма. По-специално, данните на пътниците се сегментират, което означава, че идентификационните им данни, регистрираният биометричен образец и информацията за полета се съхраняват в три различни бази данни. Тези данни се криптират с различни ключове, както по време на съхранението, така и при предаването към сървърите, извършващи съпоставянето, където впоследствие се декриптират от летищния оператор.

65. Пътниците трябва да се регистрират за всеки полет, в кратък срок преди заминаването (например 48 часа). Тази регистрация може да бъде извършена дистанционно или на терминалите на летището с подходящо ниво на достоверност по отношение на самоличността (например подходящо ниво на достоверност съгласно eIDAS). Алтернативно, регистрацията може да бъде под същата форма, както е описано в сценарий 1, като в този случай пътниците трябва да изпратят своите данни от цифровите си портфейли до летищната система в 48-часов срок преди заминаването си.

66. И в този сценарий пътниците застават пред специално контролно устройство, оборудвано с камера. След това биометричната им проба се изпраща до централен сървър на летището, който прави опит за съпоставяне на данните с тези в централната база с биометрични данни. По този начин лицата могат да бъдат идентифицирани и проверени дали действително са регистрирани за заминаващ полет (или за качването на борда на самолета, в случай че контролът се извършва при отвеждането към самолета). В зависимост от пункта за проверка е възможно да бъдат сведени до минимум данните, които се изпращат обратно към отправящия заявката администратор на пункта за проверка, например като отговор „да/не“ или като самия резултат от съпоставянето, ако е необходимо. В този случай единствено резултатът от заявката се предава на администратора на пункта за проверка и се използва от него.

---

[95] Както е онагледено от случай на употреба 3А в приложение I към искането.
[96] Както е онагледено от случай на употреба 3Б в приложение I към искането.
[97] Вж. например Становище 3/2012 на РГ 29 относно биометричните технологии, стр. 8. Вж. също точка 26 по-горе.
[98] Съображение 4 от ОРЗД. Вж. също Становище 3/2012 на РГ 29 относно биометричните технологии, стр. 8.

67. По-специално, в този сценарий пътниците се идентифицират (сравнение 1:N), където N е броят на пътниците, очаквани на летището в рамките на няколко дни. Освен това биометрично съпоставяне се извършва само при заставането на всеки пътник на предварително определени контролни пунктове на летището на заминаване, но самото обработване на данни се извършва в централен сървър, свързан с централната база данни. Периодът на съхранение в този сценарий обикновено е 48 часа и данните се заличават след заминаването на самолета.

Оценка на ЕКЗД

68. Както се припомня по-горе, обработването на биометрични данни води до повишени рискове за правата и свободите на субектите на данни[99]. По този начин всеки пропуск в сигурността на данните може да породи особено сериозни последици за субектите на данни[100]. Администраторите са длъжни да смекчат тези рискове по ефективен начин. Тъй като в този сценарий цялата архитектура е напълно централизирана, пътниците в по-голяма степен губят контрол върху своите данни. Освен това рискът данните в крайна сметка да бъдат обработени за други цели, различни от контрол на пътникопотока, също би могъл да е по-голям.

69. С оглед на принципа и изискванията за сигурност (член 5, параграф 1, буква е) и член 32 от ОРЗД) следва да се счита, че при съхраняването на идентификационни и биометрични данни в централизирани, макар и отделни бази данни, може да възникнат точки на атака, характеризиращи се с висока стойност, а нарушение на поверителността на такава база данни може впоследствие да доведе до осъществяване на достъп до целия набор от данни. Като следствие от това, евентуално нарушение, засягащо образците за лицево разпознаване и свързаните с тях идентификационни данни, може да позволи неупълномощено или неправомерно идентифициране на субектите на данни при други обстоятелства. Освен това, в зависимост от използваните методи за биометрична идентификация, е възможно това да застраши по-нататъшното безопасно използване като идентификатор на образците за лицево разпознаване. В този случай ефектите от нарушението не могат да бъдат смекчени, за разлика от други видове удостоверяване (например идентификатор на потребител, парола), които могат да се променят[101].

70. В допълнение, голямото количество и високото качество на идентификационните и биометричните данни, съхранявани от администратора, ги прави изключително ценен обект за нападатели, което означава, че от гледна точка на риска за сигурността, съществува по-голяма вероятност от атака. Освен това нарушенията на данните биха могли да пораждат по-голямо въздействие, тъй като поради съхранението на данните на централизирано място би могло да е по-лесно нападателите да получат достъп до личните данни на множество пътници. Поради това евентуалното нарушение потенциално би могло да изложи голям брой субекти на данни

[99] Вж. точка 26 по-горе.
[100] Насоки относно лицевото разпознаване, Консултативен комитет на Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни, юни 2021 г., стр. 22.
[101] Вж. в тази връзка Становище 3/2012 на РГ 29 относно биометричните технологии, стр. 34.

на сериозни рискове, например кражба на самоличност в голям мащаб, които е изключително трудно да бъдат смекчени.

71. Поради това, що се отнася до съвместимостта с член 5, параграф 1, буква е) и член 32 от ОРЗД, предвидените в сценарий 3.1 мерки[102] не са достатъчни за гарантиране на подходящо за риска ниво на сигурност с оглед на съвременното технологично равнище. Въз основа на това обработването в сценарий 3.1 няма да отговаря на член 5, параграф 1, буква е) и член 32 от ОРЗД, ако администраторът се ограничи само до тези мерки.

72. С оглед на принципа, залегнал в член 5, параграф 1, буква д) от ОРЗД, в този сценарий периодът на съхранение на биометрични данни в централната база данни обичайно е 48 часа. Това ограничаване на съхранението изглежда значително намалява рисковете, свързани с нарушения на сигурността на личните данни. Независимо от това, периодът на съхранение на данните сам по себе си не е решаващ фактор за цялостната съвместимост на въпросната архитектура, тъй като тези периоди на съхранение може да подлежат на промени от администраторите. Във всеки случай, предложените мерки трябва да отговарят на изискванията за защита на данните на етапа на проектирането и по подразбиране съгласно член 25 от ОРЗД.

73. За разлика от сценарии 1 и 2, в които се удостоверява автентичността на пътниците, в сценарий 3.1 пътниците се идентифицират (сравнение 1:N), където N е броят на пътниците, очаквани на летището в срок от няколко дни, които са дали съгласие за такова обработване при преминаването през конкретни пунктове за проверка на летището. Това предполага извършването на търсене на пътници в централна база данни чрез обработване на всяка заснета биометрична проба, за да се провери дали съвпада с известно на системата лице. За разлика от сценарий 2, в сценарий 3.1 ключовете не са достъпни единствено за пътника. Като последица от това, пътниците разполагат със значително по-малко контрол върху биометричните си данни. Следователно това обработване, както е предложено съгласно сценарий 3.1, не може да бъде съвместимо с изискванията за защита на данните на етапа на проектирането и по подразбиране съгласно член 25 от ОРЗД.

74. С оглед на член 25 от ОРЗД администраторите следва да вземат предвид видовете, категориите и нивото на подробност на личните данни, необходими за целите на обработването[103]. Когато събират големи обеми лични данни, на етапа на проектирането те трябва да отчетат увеличения риск за принципите на свеждане на данните до минимум, цялостност и поверителност и ограничение на съхранението, и да го сравнят с намаления риск при събиране на намалени обеми и/или не толкова подробна информация за субектите на данни. Във всеки случай настройката по подразбиране не трябва да включва събиране на лични данни, които не са необходими за конкретната цел на обработването. Казано по друг начин, ако не са необходими определени категории лични данни или подробни данни, тъй като са достатъчни данни, които не са толкова подробни, не следва да се събират ненужни лични данни. Ако в този случай

[102] Както е описано в точки 64—67 по-горе.

[103] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране, точка 49.

прилагането на друго обработване би могло да постигне същата цел и е достъпно съгласно условията, описани в сценарий 3.1, не е необходимо да се използва технология за лицево разпознаване.

75. Що се отнася до член 25 от ОРЗД, ключов елемент на защитата на данните на етапа на проектирането и по подразбиране е автономността на субекта на данни. По-специално субектът на данните следва да се ползва с възможно най-висока степен на автономност при определянето на начините, по които да се използват неговите лични данни, както и по отношение на обхвата и условията на това използване или обработване[104]. В сценарий 1 субектът на данни разполага с автономност и контрол по отношение на използването, разкриването и изтриването на биометричните си образци, а в сценарий 2 физическото лице запазва известен контрол по отношение на разкриването на своя собствен биометричен образец, тъй като то съхранява криптографския ключ/тайната. В сценарий 3.1 обаче лицето зависи изцяло от решенията на администратора по отношение на обработването на своите биометрични данни, поради което не разполага с пряк контрол по отношение на използването на своя биометричен образец.

76. Що се отнася до съвместимостта с член 25 от ОРЗД, и по-специално с цел да се спази изискването за свеждане на данните до минимум, предвиденото в сценарий 3.1 обработване не може да отговори на принципа на необходимост. Комитетът счита, че подобен резултат за рационализиране на пътникопотока на летищата може да бъде постигнат по начин, който представлява по-малка намеса в неприкосновеността на личния живот. Това може да бъде постигнато например без да се използват биометрични данни (въпреки че в такъв случай преживяванията на ползвателя биха били различни, тъй като е възможно да отнеме повече време да покаже бордната си карта и, при необходимост, официалните си идентификационни документи). Освен това други решения, по-специално свързани със съхраняването на биометрични данни в цифровия портфейл на място в устройството на лицето или налагащи криптиране на данните със специален ключ, съхраняван в устройството на лицето, позволяват постигането на целите по начин, който представлява по-малка намеса в неприкосновеността на личния живот.

77. Що се отнася до принципа на пропорционалност, предвиденото в сценарий 3.1 обработване поражда рискове за правата на субектите на данни, които с оглед на съвременното технологично равнище няма да бъдат смекчени от предвидените мерки. Рискът от отрицателно въздействие върху основните права и свободи на субектите на данни, което би могло да възникне в резултат на нарушение на данните в централизирана база данни, съдържаща биометричните данни на голям брой лица, изглежда надхвърля очакваните ползи от обработването, тъй като тези ползи са относително незначителни, т.е. леко увеличение на удобството и бързината на проверките. Поради това те не могат да оправдаят високата степен на намеса на тези мерки в основните права и свободи на лицата, а предвиденото в сценарий 3.1 обработване не отговаря на принципа на пропорционалност.

[104] Насоки № 4/2019 на ЕКЗД относно защитата на данните на етапа на проектирането и по подразбиране, точка 70. В съображение 7 от ОРЗД допълнително се пояснява, че „[ф]изическите лица следва да имат контрол върху собствените си лични данни“.

78. С оглед на тези съображения, в отговор на въпрос 2.2.1 Комитетът заключава, че когато обработването се извършва с конкретната цел да се рационализира пътникопотока на летищата, предвиденото в сценарий 3.1 обработване:

- **не може да бъде съвместимо с член 25 от ОРЗД**;
- **не би отговаряло на член 5, параграф 1, буква е) и член 32 от ОРЗД,** ако администраторът се ограничи до описаните в сценарий 3.1 мерки.

3.2.3.2 Сценарий 3.2: централизирано съхранение в облак, под контрола на авиокомпанията

Описание на сценария

79. В сценарий 3.2 регистрираните биометрични образци на пътниците се съхраняват в облака под контрола на авиокомпанията или на доставчика ѝ на компютърни услуги „в облак“ (обработващ лични данни). В искането се посочва, че доставчикът на компютърни услуги „в облак“ е разположен в ЕИП[105]. В този случай данните на пътниците се криптират, но се декриптират, когато се използват (например при извършване на операцията по съпоставяне), а ключовете се контролират от авиокомпанията или от назначения от нея обработващ лични данни „в облак“. Биометричните данни на пътниците се използват за идентифициране на пътниците (сравнение 1:N), където N потенциално стига до броя на всички клиенти на авиокомпанията[106].

80. Подобно на сценарии 1, 2 и 3.1, и в този случай пътниците трябва първо да се регистрират. В сценарий 3.2 обаче регистрацията на пътниците се извършва еднократно за целия период, в който клиентът разполага с профил в авиокомпанията. Регистрацията се извършва в дистанционен режим с подходящо ниво на достоверност по отношение на самоличността (например подходящо ниво на достоверност съгласно eIDAS) или на терминалите на летището. Биометрично съпоставяне се извършва само при заставането на пътниците на предварително определени контролни пунктове на летището, но самото обработване на данните се извършва в облака.

81. На летището пътниците преминават през специални контролни устройства, оборудвани с камера. Биометричните данни на пътниците се изпращат посредством заявка до сървър на авиокомпанията, разположен в облак, в който се извършва съпоставянето на тези данни с централната база данни. По този начин пътниците могат да бъдат идентифицирани и проверени дали действително са регистрирани за заминаващ полет (или за качването на борда на самолета, в случай че контролът се извършва при отвеждането към самолета).

82. Резултатите от съпоставянето потенциално могат да бъдат предоставени на разположение на множество летищни оператори, когато авиокомпанията разполага със специален терминал или достъп до инфраструктурата на общата информационна система на летището. В зависимост от пункта за проверка е възможно да бъдат сведени до минимум данните, които се изпращат обратно към отправящия заявката администратор на пункта за проверка, например като отговор „да/не“ или като самия резултат от съпоставянето, ако е необходимо. В този случай администраторът на пункта за проверка узнава и използва единствено резултата от заявката.

---

[105] Френският НО поясни, че това е примерна ситуация и че биха могли да се предвидят и доставчици на компютърни услуги „в облак“, които не са разположени в ЕИП. Освен това биха могли да се предвидят и други решения за съхранение (например без използване на облак).

[106] Френският НО поясни, че това е примерна ситуация и че е налице решение, при което биометричните данни всеки път се изпращат преди полета.

83. Периодът на съхранение на образеца се определя от авиокомпанията и потенциално може да обхване цялото време, през което клиентът разполага с профил в авиокомпанията.

Оценка на ЕКЗД

84. Съображенията, които вече бяха изразени от Комитета във връзка със сценарий 3.1[107], важат и за настоящия сценарий.

85. Що се отнася до принципа и изискванията за сигурност (член 5, параграф 1, буква е) и член 32 от ОРЗД), обработването на данни в сценарий 3.2 се извършва в облака и множество субекти биха могли да разполагат с достъп до тези данни, което евентуално включва доставчици от държави извън ЕИП, дори когато данните се съхраняват в ЕИП[108]. Такава архитектура води до потенциални рискове, свързани с прехвърлянето на лични данни в трети държави. В допълнение, макар че данните на пътниците се криптират, те се декриптират, когато се използват (т.е. при извършване на операцията по съпоставяне), докато ключовете се контролират от авиокомпанията или от назначения от нея обработващ лични данни „в облак“. Такова съхранение може да доведе до допълнително увеличение на риска за сигурността.

86. Поради това, що се отнася до съвместимостта с член 5, параграф 1, буква е) и член 32 от ОРЗД, предвидените в сценарий 3.2 мерки[109] не са достатъчни за гарантиране на подходящо за риска ниво на сигурност с оглед на съвременното технологично равнище. Въз основа на това обработването в сценарий 3.2 няма да отговаря на член 5, параграф 1, буква е) и член 32 от ОРЗД, ако администраторът се ограничи до тези мерки.

87. Освен това съгласно сценарий 3.2[110] данните биха могли да се съхраняват за значителен период от време (т.е. който потенциално обхваща цялото време, през което субектът на данни разполага с профил в авиокомпанията). Такава продължителност на съхранението излага данните на по-големи рискове от нарушение на тяхната поверителност и цялостност и изглежда надхвърля строго необходимото и пропорционалното за целите на обработването. Комитетът отбелязва, че периодът на съхранение на данните сам по себе си не е решаващ фактор за цялостната съвместимост на въпросната архитектура с ОРЗД, тъй като той може да подлежи на промени от администраторите на данните. Въз основа обаче на информацията, с която разполага Комитетът и която се съдържа в описанието на сценарий 3.2, не е налице достатъчна обосновка за този продължителен период на задържане и няма видими мерки за смекчаване на рисковете за лицата. На тази основа предложеният период на съхранение няма да бъде ограничен до необходимото съгласно принципа за ограничение на съхранението, посочен в член 5, параграф 1, буква д) от ОРЗД.

88. Във всеки случай предложените мерки в сценарий 3.2 не могат да отговорят на изискванията за защита на данните на етапа на проектирането и по подразбиране съгласно член 25 от ОРЗД. В сценарий 3.2 регистрираните биометрични образци на пътниците се съхраняват в облака под контрола на авиокомпанията или на доставчика ѝ на компютърни услуги „в облак“ (обработващ

[107] Точки 68—77 по-горе.
[108] Координирано действие по правоприлагане на ЕКЗД за 2022 г. относно използването на базирани в облак услуги от държавния сектор, 17 януари 2023 г., стр. 19.
[109] Вж. точки 79—83 по-горе.
[110] Вж. точка 83 по-горе.

лични данни). Както е описано по-горе, множество субекти потенциално биха могли да разполагат с достъп до тези данни. Освен това биометричните данни на пътниците се използват за идентифициране на пътниците (сравнение 1:N), където N потенциално стига до броя на всички ползватели/клиенти на авиокомпанията. Такъв метод предполага намирането на даден човек измежду група хора в рамките на централна база данни чрез обработването на всяко заснето лице на пътник, за да се провери дали то съвпада с човек, известен на системата. За разлика от сценарий 3.1, в сценарий 3.2 съпоставянето би могло да се извършва в доста по-голям мащаб, тъй като тук критерият е броят на всички клиенти на авиокомпанията, докато сценарий 3.1 обхваща само броя на пътниците, очаквани на летището в рамките на няколко дни.

89. Освен това, що се отнася до съвместимостта с член 25 от ОРЗД, и по-специално с цел да се спази изискването за свеждане на данните до минимум, предвиденото в сценарий 3.2 обработване не може да отговори на принципа на необходимост. Комитетът счита, че подобен резултат за рационализиране на пътникопотока на летищата би могъл да се постигне с други мерки, които представляват по-малка намеса, например без да се използват биометрични данни, въпреки че в такъв случай преживяванията на ползвателя биха били различни, тъй като е възможно да отнеме повече време да покаже идентификационния си документ и бордната си карта. Освен това други решения, по-специално свързани със съхраняването на биометрични данни в цифровия портфейл на място в устройството на лицето или налагащи криптиране на данните със специален ключ, съхраняван в устройството на лицето, позволяват на администратора да постигне целите по начин, който представлява по-малка намеса в неприкосновеността на личния живот.

90. Що се отнася до принципа на пропорционалност, предвиденото в сценарий 3.2 обработване поражда рискове за правата на субектите на данни, които няма да бъдат смекчени от предвидените гаранции. Отрицателното въздействие върху основните права и свободи на субектите на данни, което би произтекло от нарушение на данните в централизирана база данни, съдържаща съхранявани в облака биометрични данни на голям брой лица, изглежда надхвърля очакваните ползи в резултат на обработването, тъй като тези ползи са относително незначителни, т.е. леко увеличение на удобството и бързината на проверките. Поради това те не могат да оправдаят високата степен на намеса на тези мерки в основните права и свободи на лицата, а предвиденото в сценарий 3.2 обработване не може да се счита за пропорционално.

91. С оглед на тези съображения, в отговор на въпрос 2.3.1 Комитетът заключава, че когато обработването се извършва с конкретната цел да се рационализира пътникопотока на летищата, предвиденото в сценарий 3.2 обработване:

- **не може да бъде съвместимо с член 25 от ОРЗД**;
- **не би отговаряло на член 5, параграф 1, буква е) и член 32 от ОРЗД,** ако администраторът се ограничи до описаните в сценарий 3.2 мерки;
- **не би отговаряло на член 5, параграф 1, буква д) и член 32 от ОРЗД**, тъй като въз основа на информацията, с която разполага Комитетът, няма достатъчна обосновка за предвидения в сценарий 3.2 период на съхранение. За да се спази принципът за ограничение на съхранението, посочен в член 5, параграф 1, буква д) от ОРЗД, администраторът трябва да докаже, че личните данни се съхраняват за период, не по-дълъг от необходимото за целите, за които се обработват.

4 ЗАКЛЮЧЕНИЯ

92. По отношение на въпрос 1.1, въз основа на искането за становище от Френския НО във връзка с изискванията на член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД и въз основа на анализа по-горе Комитетът заключава, че:

93. използването на технологии за лицево разпознаване за удостоверяване на автентичността с помощта на биометрични данни с конкретната цел да се рационализира пътникопотока на летищата (пунктове за проверка за сигурност, оставяне на багажа, отвеждане към самолета и влизане в салоните за пътници) принципно би могло да се счита за съвместимо с принципите на цялостност и поверителност съгласно член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД в случай на архитектура за съхранение, при която регистрираният биометричен образец на всеки пътник се съхранява на място в индивидуалното му устройство и под негов изключителен контрол, ако се прилагат подходящи гаранции, както са описани в точка 46 и сл. по-горе.

94. По отношение на въпрос 2.1.1, въз основа на искането за становище от Френския НО във връзка с изискванията на член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД и въз основа на анализа по-горе Комитетът заключава, че:

95. използването на технологии за лицево разпознаване за удостоверяване на автентичността с помощта на биометрични данни с конкретната цел да се рационализира пътникопотока на летищата (пунктове за проверка за сигурност, оставяне на багажа, отвеждане към самолета и влизане в салоните за пътници) принципно би могло да се счита за съвместимо с принципа за ограничение на съхранението съгласно член 5, параграф 1, буква д) и с принципите за цялостност и поверителност съгласно член 5, параграф 1, буква е) и членове 25 и 32 от ОРЗД в случай на архитектура за централизирано съхранение, при която регистрираният биометричен образец на всеки пътник се съхранява в централна база данни в рамките на летището под контрола на летищния оператор, в криптирана форма, с ключ/тайна, достъпни единствено за лицето, ако се прилагат подходящи гаранции, както са описани в точка 60 и сл. по-горе.

96. По отношение на въпрос 2.2.1, въз основа на искането за становище от Френския НО във връзка с изискванията на член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД и въз основа на анализа по-горе Комитетът заключава, че:

97. използването на технологии за лицево разпознаване за идентифициране с помощта на биометрични данни, използвано с конкретната цел да се рационализира пътникопотока на летищата (пунктове за проверка за сигурност, оставяне на багажа, отвеждане към самолета и влизане в салоните за пътници) в случай на архитектура за централизирано съхранение, при която регистрираните биометрични образци на пътниците не са криптирани с ключ/тайна, достъпни единствено за пътника, като тези образци се съхраняват в база данни в рамките на летището (под контрола на летищния оператор), не може да бъде съвместимо с член 25 от ОРЗД. Освен това такова обработване не би отговаряло на принципите за цялостност и поверителност съгласно член 5, параграф 1, буква е) и член 32 от ОРЗД, ако администраторът се ограничи до описаните в сценарий 3.1 мерки.

98. По отношение на въпрос 2.3.1, въз основа на искането за становище от Френския НО във връзка с изискванията на член 5, параграф 1, букви д) и е) и членове 25 и 32 от ОРЗД и въз основа на анализа по-горе Комитетът заключава, че:

99. използването на технологии за лицево разпознаване за идентифициране с помощта на биометрични данни, използвано с конкретната цел да се рационализира пътникопотока на

летищата (пунктове за проверка за сигурност, оставяне на багажа, отвеждане към самолета и влизане в салоните за пътници) в случай на архитектура за централизирано съхранение, при която регистрираните биометрични образци на пътниците не са криптирани с ключ/тайна, достъпни единствено за пътника, като тези образци се съхраняват в облака (под контрола на авиокомпанията), не може да бъде съвместимо с член 25 от ОРЗД. Освен това такова обработване не би отговаряло на принципите за цялостност и поверителност съгласно член 5, параграф 1, буква е) и член 32 от ОРЗД, ако администраторът се ограничи до описаните в сценарий 3.2 мерки. Накрая, въз основа на описанието на сценарий 3.2 и информацията, с която разполага Комитетът, обработването не би отговаряло на принципа за ограничение на съхранението съгласно член 5, параграф 1, буква д) от ОРЗД.

За Европейския комитет по защита на данните

Председател

(Anu Talus)