A Testület véleménye (64. cikk)

11/2024. sz. vélemény a repülőtéri utasforgalom egyszerűsítése érdekében az arcfelismerés alkalmazásáról (összeegyeztethetőség az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével)

1.1. verzió

Elfogadás időpontja: 2024. május 23.

Elfogadott

1.1. verzió	2024. május 28.	Nyelvtani helyesbítés az összefoglalóban (3. és 4. oldal), valamint a vélemény 77. és 90. bekezdésében
1.0. verzió	2024. május 23.	A vélemény elfogadása

Vezetői összefoglaló

A francia felügyeleti hatóság véleménykéréssel fordult az Európai Adatvédelmi Testülethez azzal kapcsolatban, hogy a repülőtér-üzembentartók és a légitársaságok hogyan használják az arcfelismerő technológiát az utasok biometrikus alapú hitelesítésére vagy azonosítására a repülőtéri utasforgalom egyszerűsítése érdekében.

Előzetes megjegyzésként a Testület emlékeztet arra, hogy a biometrikus adatok, és különösen az arcfelismerő technológia használata fokozott kockázatokkal jár az érintettek jogaira és szabadságaira nézve. Biometrikus adatok kezelésével jár, amelyek az általános adatvédelmi rendelet 9. cikke értelmében különleges védelmet élveznek. Az ilyen technológiák használata előtt – még ha azok különösen hatékonynak tekinthetők is – az adatkezelőknek fel kell mérniük az érintettek alapvető jogaira és szabadságaira gyakorolt hatást, és meg kell vizsgálniuk, hogy az adatkezelés törvényes célja elérhető-e kevésbé intruzív eszközökkel.

A jelen vélemény terjedelme – a kérelemnek megfelelően – annak vizsgálatára korlátozódik, hogy az adatkezelés összeegyeztethető-e **az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével**, ha az adatkezelés **kifejezett célja a repülőterek utasforgalmának egyszerűsítése** négy konkrét ellenőrzőponton, nevezetesen a biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor. Ez a vélemény nem tartalmaz teljes körű elemzést arról, hogy az érintett adatkezelők és adott esetben azok adatfeldolgozói minden egyes esetben megfelelnek-e az általános adatvédelmi rendeletnek. Ennélfogva ez a vélemény nem terjed ki valamely adatkezelő konkrét előirányzott adatkezelésén és körülményein alapuló, esetfüggő jogi és technikai elemzésre. Ezenkívül az alkalmazandó jogalap elemzése nem tartozik a kérelemben a Testület elé terjesztett kérdések körébe, ennélfogva a jelen vélemény nem vizsgálja az általános adatvédelmi rendelet 6., 7. és 9. cikke szerinti adatkezeléshez való hozzájárulás érvényességét. Ezenkívül a jelen vélemény nem érinti a biometrikus adatok felhasználására vonatkozóan a tagállami jogban előírt korlátozásokat.

Ebben a véleményben a Testület **négy konkrét forgatókönyv** összefüggésében értékeli, hogy az adatkezelés megfelel-e az általános adatvédelmi rendelet említett rendelkezéseinek.

Az **első forgatókönyv** szerint az utast a nála, például személyes eszközén tárolt, kizárólagos ellenőrzése alatt lévő regisztrált biometrikus sablonnal hitelesítik (1:1 összehasonlítással) az említett repülőtéri ellenőrzőpontokon való áthaladáskor.

A Testület arra a következtetésre jut, hogy a választott intézkedések akkor felelnek meg a szükségesség elvének, ha az adatkezelő bizonyítani tudja, hogy nincsenek olyan kevésbé intruzív alternatív megoldások, amelyekkel ugyanaz a cél hatékonyan elérhető. Emellett az adatkezelés intruzív jellegét ellensúlyozhatja az utasok aktív részvétele, mivel biometrikus sablonjuk tárolása kizárólag náluk, például a kizárólagos ellenőrzésük alatt lévő személyes eszközükön történik, és adataikat röviddel a megfeleltetés befejezése után törlik. Ennek alapján a Testület arra a következtetésre jut, hogy az első forgatókönyvben előirányzott adatkezelés **elvben összeegyeztethetőnek tekinthető az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával, valamint 25. és 32. cikkével**, ennek feltétele a megfelelő biztosítékok érvényesítése.

A Testület biztosítékokat határozott meg, amelyeket minimum követelményként érvényesíteni kell az első forgatókönyvhöz hasonló megoldás esetén.

A **második forgatókönyv** szerint a regisztrált biometrikus sablont a repülőtéren központosítottan tárolják titkosított formában, amelyhez kizárólag az utasnál lévő kulcs vagy titkos adat tartozik. Ez lehetővé teszi az utasok hitelesítését (1:1 összehasonlítás) a fent említett repülőtéri ellenőrző pontokon való áthaladás során. A regisztráció meghatározott időtartamra érvényes, amely lehet például az utolsó úttól számított egy év, vagy az útlevél érvényességi ideje.

A Testület arra a következtetésre jut, hogy az adatkezelés akkor feleltethető meg a szükségesség elvének, ha az adatkezelő bizonyítani tudja, hogy nincsenek olyan kevésbé intruzív alternatív megoldások, amelyekkel ugyanaz a cél hatékonyan elérhető. Emellett az adatkezelés intruzív jellegét ellensúlyozhatja az utasok aktív részvétele, akik kizárólagos ellenőrzésük alatt tartják a titkosított biometrikus adataikhoz tartozó kulcsot vagy titkos adatot. Feltételezve, hogy az adatkezelő megfelelő biztosítékokat érvényesít, a központosított adatbázis e forgatókönyv szerinti használatából eredő biztonsági kockázatok csökkenthetők, és az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás a várható előnyhöz képest arányosnak tekinthető. Ami a korlátozott tárolhatóság elvét illeti, a Testület nem kapott az adattárolás hosszú időtartamát alátámasztó információkat. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontjával való összeegyeztethetőség elérése érdekében az adatkezelőknek meg kell tudniuk indokolni, hogy a konkrét esetekben miért van szükség az előirányzott adatmegőrzési időre. A Testület azt ajánlja, hogy az adatkezelők a lehető legrövidebb adattárolási időtartamot irányozzák elő, ugyanakkor kínálják fel az utasoknak azt a lehetőséget, hogy meghatározzák az általuk preferált adattárolási időtartamot. Ennek alapján a Testület arra a következtetésre jut, hogy a második forgatókönyvben előirányzott adatkezelés **elvben összeegyeztethetőnek tekinthető az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével**, ennek feltétele a megfelelő biztosítékok érvényesítése.

A Testület biztosítékokat határozott meg, amelyeket minimum követelményként érvényesíteni kell a második forgatókönyvhöz hasonló megoldás esetén.

A **harmadik forgatókönyv** a regisztrált biometrikus sablon titkosított formában, a repülőtéren belül történő központosított tárolását jelenti, a repülőtér-üzembentartó ellenőrzése alatt . Ez lehetővé teszi az utasok azonosítását (1:N összehasonlítás) a fent említett repülőtéri ellenőrző pontokon való áthaladás során. Ebben a forgatókönyvben az adattárolás időtartama jellemzően 48 óra, és az adatokat a repülőgép felszállását követően törlik.

Mivel a személyazonosító és biometrikus adatok tárolása egy központi adatbázisban történik, ha sérül az adatbázis titkossága, az később a teljes adatkészlethez való hozzáférést eredményezheti, és lehetővé teheti az utasok jogosulatlan vagy jogellenes azonosítását más környezetben. A repülőtér-üzembentartó ellenőrzése alatt álló központosított tárolási architektúra révén továbbá az utasok nagyobb mértékben veszítik el adataik feletti rendelkezést. A Testület úgy véli, hogy a repülőtéri utasforgalom egyszerűsítéséhez hasonló eredmény kevésbé intruzív módon is elérhető, és az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás, amely a biometrikus adatok központosított adatbázisában előforduló adatvédelmi incidensből eredne, feltehetően meghaladja az adatkezeléstől várható előnyt. Ezért az adatkezelés nem felel meg a szükségesség és az arányosság elvének. Ennek alapján a Testület megállapítja, hogy a harmadik forgatókönyvben előirányzott adatkezelés **nem tekinthető összeegyeztethetőnek az általános adatvédelmi rendelet 25. cikkével**. Továbbá **nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának és 32. cikkének**, ha az adatkezelő az ebben a forgatókönyvben leírt intézkedésekre szorítkozna.

A **negyedik forgatókönyv** szerint a regisztrált biometrikus sablont titkosított formában, a légitársaság vagy felhőszolgáltatója ellenőrzése alatti felhőben központosítottan tárolják. Ez lehetővé teszi az utasok azonosítását (1:N összehasonlítás) a fent említett repülőtéri ellenőrző pontokon való áthaladás

során. Ebben a forgatókönyvben az adattárolás időtartama potenciálisan addig terjedhet, amíg az ügyfél fiókkal rendelkezik a légitársaságnál.

Mivel a személyazonosító és biometrikus adatok tárolása a felhőben található központi adatbázisban történik, az adatok több szervezet – köztük esetleg az EGT-n kívüli szolgáltatók – számára is hozzáférhetővé válhatnak. Az utas adatait használat közben dekódolják, a kulcsok pedig a légitársaság vagy annak adatfeldolgozói ellenőrzése alatt állnak, ami növelheti a biztonsági kockázat felületét. A központosított tárolási architektúra révén továbbá az utasok nagyobb mértékben veszítik el adataik feletti rendelkezést. Emellett az adatok jelentős ideig tárolhatók, ami az adatok tekintetében a biztonság sérelmének nagyobb fokú kockázatával jár, és feltehetően meghaladja az adatkezelés céljából feltétlenül szükséges és arányos mértéket, kivéve, ha további látható intézkedéseket hoznak az egyéneket érintő kockázatok csökkentése érdekében.

A Testület úgy véli, hogy a repülőtéri utasforgalom egyszerűsítéséhez hasonló eredmény kevésbé intruzív módon is elérhető, és az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás, amely a biometrikus adatok központosított adatbázisában előforduló adatvédelmi incidensből eredhet, feltehetően meghaladja az adatkezeléstől várható előnyt. Ezért az adatkezelés nem felel meg a szükségesség és az arányosság elvének. Ennek alapján a Testület megállapítja, hogy a negyedik forgatókönyvben előirányzott adatkezelés **nem tekinthető összeegyeztethetőnek az általános adatvédelmi rendelet 25. cikkével**. Továbbá **nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése e) pontjának** a Testület rendelkezésére álló információk alapján, és **nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának és 32. cikkének**, ha az adatkezelő az ebben a forgatókönyvben leírt intézkedésekre szorítkozna.

Tartalomjegyzék

Az Európai Adatvédelmi Testület,

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: **általános adatvédelmi rendelet**) 63. cikkére és 64. cikkének (2) bekezdésére,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[1],

tekintettel az Európai Adatvédelmi Testület (a továbbiakban: **a Testület**) eljárási szabályzatának (a továbbiakban: **a Testület eljárási szabályzata**) 10. és 22. cikkére,

mivel:

(1) A Testület fő feladata az általános adatvédelmi rendelet következetes alkalmazásának biztosítása az Európai Gazdasági Térség (a továbbiakban: **EGT**) egész területén. Az általános adatvédelmi rendelet 64. cikkének (2) bekezdése úgy rendelkezik, hogy bármely felügyeleti hatóság, a Testület elnöke vagy a Bizottság kérheti, hogy a Testület vizsgáljon meg egy általános érvényű vagy egynél több EGT-tagállamban hatással bíró ügyet, és bocsásson ki róla véleményt.

(2) A Testület véleményét az általános adatvédelmi rendelet 64. cikkének (3) bekezdése és Testület eljárási szabályzata azzal együtt értelmezett 10. cikkének (2) bekezdése alapján nyolc héten belül kell elfogadni azt követően, hogy az elnök és az illetékes felügyeleti hatóság határozatban megállapította az akta hiánytalanságát. Az ügy összetettségére figyelemmel ez a határidő az elnök döntésével további hat héttel meghosszabbítható,

a következő véleményt fogadta el:

1 BEVEZETÉS

1.1 A tényállás

1. 2024. február 16-án a francia felügyeleti hatóság véleménykéréssel fordult a Testülethez azzal kapcsolatban, hogy összeegyeztethető-e az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével, ha a repülőtér-üzembentartók és a légitársaságok arcfelismerő technológiát használnak az utasok biometrikus alapú hitelesítésére vagy azonosítására[2]

[1] Az e véleményben a „**tagállamokra**” való hivatkozásokat az „EGT-tagállamokra” való hivatkozásként kell érteni. Ebben a véleményben az Unióra való hivatkozást az EGT-re történő hivatkozásként kell érteni.

[2] A jelen vélemény összefüggésében „**utas**” az olyan érintett, akinek a személyes adatait a jelen véleményben ismertetett konkrét célból kezelik. A továbbiakban ebben a véleményben az „utas” és az „egyén” fogalmak egymással felcserélhetők.

annak érdekében, hogy a repülőtéri biztonsági ellenőrzőpontokon[3], a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor (ide nem értve a határellenőrzést és a vámmentes üzletek által végzett ellenőrzéseket) egyszerűsítsék a repülőtéri utasforgalmat (a továbbiakban: a **kérelem**). A francia felügyeleti hatóság a kérelméhez csatolta a jellemző alkalmazási esetek leírását (I. melléklet).

2. Kérelmében a francia felügyeleti hatóság rámutat, hogy a jelenleg több uniós repülőtéren tesztelt modellek tagállamonként eltérnek, emiatt pedig felmerülhet a felügyeleti hatóságok általi eltérő értelmezések kockázata, valamint annak kockázata, hogy az érintettek alapvető jogait és szabadságait érintően különböző kihatások jelentkeznek az EU-ban[4].

3. A Testület úgy véli, hogy a kérelemre adandó válaszhoz a következő kérdéseket kell megválaszolni:

4. **1. kérdés**:

1.1. Összeegyeztethető-e **az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával, valamint 25. és 32. cikkével** az arcfelismerő technológia biometrikus alapú hitelesítésre történő alkalmazása **a repülőtéri utasforgalom egyszerűsítésének konkrét céljából** (a biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor) olyan tárolási architektúra esetében, ahol az egyes utasok biometrikus sablonját **kizárólag az adott egyénnél**, például annak kizárólagos ellenőrzése alatt lévő (személyes) eszközén tárolják?

1.2. Amennyiben megállapítást nyer, hogy az ilyen célú adatkezelés összeegyeztethető az említett rendelkezésekkel, minimálisan milyen megfelelő biztosítékokra lenne szükség az általános adatvédelmi rendelet 25. és 32. cikkének fényében?

2. kérdés:

2.1. Összeegyeztethető-e **az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével** az arcfelismerő technológia biometrikus alapú hitelesítésre vagy azonosításra, **a repülőtéri utasforgalom egyszerűsítésének konkrét céljából** (a biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor) történő alkalmazása olyan **központosított** tárolási architektúra esetében, ahol az egyes utasok biometrikus sablonját központi adatbázisban tárolják:

2.1.1. A repülőtéren belül, a repülőtér-üzembentartó ellenőrzése alatt álló központi adatbázisban, titkosított formában, kizárólag az egyénnél (például a mobiltelefonjában) tárolt kulccsal vagy titkos adattal, hitelesítés céljából?

2.1.2. Amennyiben megállapítást nyer, hogy az ilyen célú adatkezelés összeegyeztethető, minimálisan milyen megfelelő biztosítékokra lenne szükség az általános adatvédelmi rendelet 25. és 32. cikkének fényében?

[3] A jelen vélemény alkalmazásában a „**repülőtéri biztonsági ellenőrzőpontok**" a repülőtér-üzembentartó felelőssége mellett végzett azon biztonsági ellenőrzéseket jelentik, amelyeken az utasoknak át kell esniük ahhoz, hogy az indulási csarnokból bejuthassanak a beszállóterületre vagy a beszállókapuhoz.
[4] Kérelem, 1. o.

2.2.1. A repülőtéren belül, a repülőtér-üzembentartó ellenőrzése alatt álló központi adatbázisban, titkosított formában, a repülőtér-üzembentartónál lévő kulcsokkal, azonosítás céljából?

2.2.2. Amennyiben megállapítást nyer, hogy az ilyen célú adatkezelés összeegyeztethető, minimálisan milyen megfelelő biztosítékokra lenne szükség az általános adatvédelmi rendelet 25. és 32. cikkének fényében?

2.3.1. A felhőben, a légitársaság vagy szolgáltatója (adatfeldolgozó) ellenőrzése alatt, titkosított formában, a légitársaságnál vagy szolgáltatójánál lévő kulcsokkal, azonosítás céljából?

2.3.2. Amennyiben megállapítást nyer, hogy az ilyen célú adatkezelés összeegyeztethető, minimálisan milyen megfelelő biztosítékokra lenne szükség az általános adatvédelmi rendelet 25. és 32. cikkének fényében?

5. Miután a francia felügyeleti hatóság teljesnek tekintette az ügyiratot 2024. február 16-án, és 2024. február 23-án a Testület elnöke is megállapította az ügyirat teljességét, a Titkárság 2024. február 23-án körbeküldte az iratokat. A Testület elnöke az általános adatvédelmi rendeletnek az Európai Adatvédelmi Testület eljárási szabályzata 10. cikkének (2) bekezdésével összefüggésben értelmezett 64. cikkének (3) bekezdésével összhangban úgy határozott, hogy az ügy tárgyának összetettsége miatt hat héttel meghosszabbítja az alapértelmezett nyolchetes határidőt.

1.2 Az általános adatvédelmi rendelet 64. cikkének (2) bekezdése szerinti vélemény iránti kérelem elfogadhatósága

6. Az általános adatvédelmi rendelet 64. cikkének (2) bekezdése úgy rendelkezik, hogy bármely felügyeleti hatóság kérheti, hogy a Testület vizsgáljon meg egy általános érvényű vagy egynél több tagállamban hatással bíró ügyet, és bocsásson ki róla véleményt.

7. A Testület úgy véli, hogy a francia felügyeleti hatóság által az arcfelismerő technológia biometrikus alapú hitelesítésre vagy azonosításra, a repülőtéri utasforgalom egyszerűsítésének konkrét céljából történő alkalmazásának összeegyeztethetőségével kapcsolatban előterjesztett kérelem „egynél több tagállamban hatással bíró” kérdéseket érint, mivel – amint azt a kérelem kifejti[5] – jelenleg több projekt megvalósítása zajlik a tagállamok repülőterein, és a becslések szerint az ilyen célú felhasználás az elkövetkező években növekedni fog. A különböző repülőterek és légitársaságok által jelenleg tesztelt modellek tagállamonként jelentősen eltérnek, emiatt pedig felmerülhet az a kockázat, hogy adatvédelmi szempontból eltérő hatások fognak kialakulni egynél több tagállamban.

8. A Testület továbbá úgy véli, hogy a francia felügyeleti hatóság által előterjesztett kérelem jelentős következményekkel jár az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjában meghatározott elvek, az általános adatvédelmi rendelet 25. cikke alapján az adatkezelőkre alkalmazandó követelmények, valamint az általános adatvédelmi rendelet 32. cikke alapján az adatkezelőkre és az adatfeldolgozókra alkalmazandó követelmények alkalmazására nézve. Ezért ez a kérelem az általános adatvédelmi rendelet 64. cikkének (2) bekezdése értelmében vett „általános érvényű ügyre” vonatkozik, mivel a korlátozott tárolhatóság (az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontja), valamint az integritás és bizalmas jelleg (az általános adatvédelmi

[5] Kérelem, 3. o.

rendelet 5. cikke (1) bekezdésének f) pontja) elveinek, valamint a beépített és alapértelmezett adatvédelem (az általános adatvédelmi rendelet 25. cikke) és az adatbiztonság (az általános adatvédelmi rendelet 32. cikke) fogalmainak következetes értelmezését érinti, amelynek célja többek között a felsorolt rendelkezések EGT-n belüli következetes alkalmazásának biztosítása.

9. Az általános adatvédelmi rendelet 5. cikke (1) bekezdése e) és f) pontjának, valamint 25. és 32. cikkének értelmezésével kapcsolatban a tagállamok között esetlegesen eltérő álláspontok növelnék annak kockázatát, hogy a repülőtér-üzembentartók és a légitársaságok eltérő módon dolgoznak ki arcfelismerő projekteket. Mivel a francia felügyeleti hatóság bizonyította, hogy az arcfelismerő technológia biometrikus alapú hitelesítésre vagy azonosításra, a repülőtéri utasforgalom egyszerűsítésének konkrét céljából történő alkalmazása kapcsán egyértelműen szükség van e rendelkezések következetes értelmezésére[6], a Testület úgy véli, hogy a kérelem az Európai Adatvédelmi Testület eljárási szabályzata 10. cikkének (3) bekezdésével összhangban alapos.

10. Az általános adatvédelmi rendelet 64. cikkének (3) bekezdése szerint az Európai Adatvédelmi Testület nem bocsát ki véleményt, ha ugyanazon ügyről már bocsátott ki véleményt[7]. Az Európai Adatvédelmi Testület még nem adott választ a kérelemből eredő kérdésekre. Bár az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása[8] már tartalmaz hasznos elemeket a biometrikus adatok kezelésére alkalmazandó biztonsági intézkedésekkel kapcsolatban, azok nem terjednek ki a kérelemben felvetett kérdésekkel kapcsolatos valamennyi szempontra. Továbbá, az Európai Adatvédelmi Testület rendelkezésre álló iránymutatásai, így az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása sem ad konkrét támpontot az utasoknak a repülőtéri utasforgalom egyszerűsítése érdekében történő azonosítására vagy hitelesítésére szolgáló biometrikus adatok központosított vagy decentralizált tárolásával kapcsolatban ellenőrizendő lehetséges elemekről, valamint az ilyen adatkezelésnek az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével való összeegyeztethetőségéről.

11. Ezen okok miatt a Testület úgy véli, hogy a kérelem elfogadható, és az abban felvetett kérdéseket az általános adatvédelmi rendelet 64. cikkének (2) bekezdése alapján elfogadott véleményben kell elemezni.

2 A VÉLEMÉNY VIZSGÁLATI KÖRE ÉS HÁTTERE

2.1 A vélemény vizsgálati köre

12. Ez a vélemény kizárólag arra vonatkozik, hogy az arcfelismerő technológiáknak a repülőtér-üzemeltetők és a légitársaságok általi, az utasok biometrikus alapú hitelesítésére vagy azonosítására, **a repülőtéri utasforgalom egyszerűsítésének konkrét céljából** (a biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor) történő, a kérelemben foglaltak szerinti alkalmazása összeegyeztethető-e az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével.

---

[6] Kérelem, 1–3. o.

[7] Az általános adatvédelmi rendelet 64. cikkének (3) bekezdése és az Európai Adatvédelmi Testület eljárási szabályzata 10. cikkének (4) bekezdése.

[8] Az Európai Adatvédelmi Testület 2020. január 29-én elfogadott 3/2019. sz. iránymutatása a személyes adatok videoeszközökkel történő kezeléséről, 2.0. verzió (a továbbiakban: **az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása**).

13. **E vélemény vizsgálati körét** illetően a Testület a következőket kívánja pontosítani:

1) A személyes adatoknak a határellenőrzések és a vámmentes üzletek által végzett ellenőrzések keretében történő kezelése nem tartozik e vélemény vizsgálati körébe, mivel azokat a repülőtér-üzemeltetőktől és a légitársaságoktól eltérő adatkezelők végzik.

2) E vélemény vizsgálati köre ugyancsak nem terjed ki az arcfelismerő technológia bármely más (például bűnüldözési) célra vagy más fél által – akár hasonló célokra – történő használatára még akkor sem, ha az a 3.2. szakaszban ismertetett forgatókönyvek alapján történik.

3) A jelen vélemény csak az utasok személyes adatainak kezelését vizsgálja, és nem terjed ki az érintettek más típusaira, például a repülőtér-üzemeltetők vagy a légitársaságok személyzetére.

4) Ez a vélemény a francia felügyeleti hatóság által benyújtott kérelmet vizsgálja a tekintetben, hogy az utasok biometrikus sablonjainak tárolási architektúrái összeegyeztethetők-e az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével. E körben ez a vélemény nem tartalmaz teljes körű elemzést arról, hogy az érintett adatkezelők és adott esetben azok adatfeldolgozói minden egyes esetben megfelelnek-e az általános adatvédelmi rendeletnek. Ez különösen fontos arra tekintettel, hogy ezek a technológiák fokozott kockázatokkal járnak a különleges adatkategóriáknak az általános adatvédelmi rendelet 9. cikke szerinti kezeléséhez kapcsolódóan. Ennélfogva ez a vélemény nem terjed ki az arcfelismerő technológiák – többek között a kérelem által érintett konkrét ágazatban történő – használatának az általános adatvédelmi rendelet egyéb rendelkezései szerinti értékelésére, sem pedig valamely adatkezelő konkrét előirányzott adatkezelésén és körülményein alapuló, esetfüggő jogi és technikai elemzésre.

5) A vélemény nem vizsgálja a gyermekek személyes adatainak kezelését, és nem érinti az e tekintetben alkalmazandó konkrét követelményeket.

6) A vélemény nem érinti a tagállamok nemzeti jogszabályaiból eredő, a biometrikus adatok felhasználására vonatkozó jogi követelményeket és további korlátozásokat[9].

7) E vélemény következtetései nem veszik figyelembe a további technológiai fejlesztéseket.

[9] Az általános adatvédelmi rendelet 9. cikkének (4) bekezdése például úgy rendelkezik, hogy a tagállamok további feltételeket – köztük korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a biometrikus adatok kezelésére vonatkozóan.

8) Ez a vélemény négy forgatókönyvet vizsgál, amelyek sajátos jellemzőit az alábbi 3.2. szakasz ismerteti. Más forgatókönyvekkel azonos célú adatkezelés esetén sem foglalkozik.

14. Kérelmében a francia felügyeleti hatóság jelezte, hogy az utasok biometrikus adatainak a repülőtéri utasforgalom egyszerűsítése céljából történő kezelése azon a feltételezésen alapulna, hogy az egyének hozzájárulnak az ilyen adatkezeléshez, ami megteremtheti az általános adatvédelmi rendelet szerinti jogalapot[10]. **Az alkalmazandó jogalap elemzése azonban nem tartozik a kérelemben a Testület elé terjesztett kérdések körébe, ennélfogva a jelen vélemény nem vizsgálja az adatkezeléshez való hozzájárulás érvényességét az általános adatvédelmi rendelet 6., 7. és 9. cikke szerint.**

15. Mindazonáltal az Európai Adatvédelmi Testület általánosságban megjegyzi, hogy ha az érintett adatkezelők erre a jogalapra támaszkodnának, akkor be kellene beszerezniük azon egyének érvényes kifejezett hozzájárulását[11], akik hajlandók igénybe venni e szolgáltatásokat. Az ilyen kifejezett hozzájárulásnak önkéntesnek és konkrétnak kell lennie, és megfelelő tájékoztatáson kell alapulnia[12]; e feltételek teljesülését eseti alapon kell vizsgálni. Ez többek között a következőket jelenti:

1) Az egyének számára lehetővé kell tenni, hogy bármikor és minden hátrány nélkül, egyszerűen visszavonhassák az adott hozzájárulást[13].

2) A hozzájárulás akkor önkéntes, ha a biometrikus alapú technológiák említett használatára kizárólag önkéntes alapon kerül sor, mivel az egyének számára lehetővé kell tenni, hogy szabadon – mindenféle hátrány (például a hozzájárulást nem adó utasok esetében jelentősen hosszabb késleltetés[14]), ösztönző, többletköltség vagy viszonzásul nyújtott további előny[15] nélkül – döntsenek az adott szolgáltatások igénybevételéről.

3) Kifejezett hozzájárulást kell kérni továbbá azon egyénektől, akiknek biometrikus adatait kezelik, még akkor is, ha nem regisztráltak ilyen módon történő azonosításra vagy hitelesítésre. Más szóval alapvető fontosságú, hogy ne készüljön kamerafelvétel azon egyének arcáról, akik nem járultak hozzá kifejezetten a tervezett célból történő

[10] Kérelem, I. melléklet.

[11] Az általános adatvédelmi rendelet 4. cikkének 14. pontja és 9. cikkének (1) bekezdése, valamint 9. cikke (2) bekezdésének a) pontja szerint tilos a biometrikus adatoknak a természetes személyek egyedi azonosítása céljából történő kezelése, kivéve, ha az érintett kifejezetten hozzájárult e személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy a tagállami jog úgy rendelkezik, hogy az általános adatvédelmi rendelet 9. cikkének (1) bekezdésében említett tilalom nem oldható fel az érintett hozzájárulásával. Lásd még az általános adatvédelmi rendelet (51), (52) és (53) preambulumbekezdését.

[12] A GDPR 4. cikkének 11. pontja és 7. cikke.

[13] Az általános adatvédelmi rendelet 7. cikkének (4) bekezdése, valamint (50) preambulumbekezdése.

[14] Ennek körében fontolóra vehető például egy olyan rendszer kialakítása, amely mentesíti a hozzájárulni nem kívánó utasokat a társadalmi nyomástól azáltal, hogy a választásuk nem érinti hátrányosan a többi utast.

[15] Az Európai Adatvédelmi Testület 2020. május 4-én elfogadott, az (EU) 2016/679 rendelet szerinti hozzájárulásról szóló 5/2020. sz. iránymutatásának 1.1. verziója (a továbbiakban: **az Európai Adatvédelmi Testület hozzájárulásról szóló 5/2020. sz. iránymutatása**), 46. és 48. pont.

arcfelismeréshez. Ez például úgy érhető el, hogy külön sávokat alakítanak ki az arcfelismeréshez, amelyeket megfelelő jelzések és fizikai elkülönítés útján egyértelműen azonosítva biztosítják a megkülönböztetést a nem biometrikus ellenőrzési forgalomtól.

4) Attól függetlenül, hogy a hozzájárulás lenne-e az ilyen adatkezelésre alkalmazandó jogalap, az adatkezelésnek az általános adatvédelmi rendelet 5. cikkében a szükségesség és az arányosság tekintetében rögzített elvei akkor is alkalmazandók, ha az egyének kifejezett hozzájárulásukat adták biometrikus adataik felhasználásához[16].

16. A kérelem meghatározza[17], hogy a repülőtér-üzembentartók a repülőtéri biztonsági ellenőrzőpontokon, míg a légitársaságok a poggyászfelvételkor, beszálláskor, valamint a várókba történő belépéskor végzett adatkezelés tekintetében járnának el adatkezelőként. A Testület megjegyzi ezért, hogy a kérelemben leírt adatkezelésben több szereplő is részt vehet, és nem mérlegelte a (közös) adatkezelő és/vagy adatfeldolgozó szerepkör alkalmazását a vélemény 3.2. pontjában ismertetett forgatókönyvek esetében. Az érintett szereplőket minden esetben azonosítani kell, és a felelősségi körüket egyértelműen meg kell jelölni az általános adatvédelmi rendelet követelményeinek történő megfelelés érdekében.[18].

17. A Testület megjegyzi továbbá, hogy az Unióban jelenleg nincs egységes jogszabályi követelmény a repülőtér-üzemeltetők és a légitársaságok számára arra vonatkozóan, hogy a fent említett ellenőrzőpontok mindegyikén azonosítsák az utasokat, és ellenőrizzék, hogy az adott utas beszállókártyáján szereplő név megegyezik-e a személyazonosító okmányában szereplő névvel[19]. Így az erre vonatkozó követelményeket a nemzeti jogszabályok írják elő, amelyek tagállamonként eltérőek lehetnek. Egyes tagállamokban az ellenőrzés kötelező egyes ellenőrzőpontok esetében (pl. poggyászfelvételkor vagy beszálláskor), míg más tagállamokban azt jelenleg nem követelik meg[20]. Az

[16] Ugyanott, 5. pont.
[17] Kérelem, I. melléklet.
[18] Az általános adatvédelmi rendelet 4. cikkének 7. és 8. pontjával, 5. cikkének (2) bekezdésével, valamint 24., 26., 28. és 29. cikkével összhangban. Lásd még az Európai Adatvédelmi Testület 7/2020. sz. iránymutatását az adatkezelő és az adatfeldolgozó általános adatvédelmi rendeletben meghatározott fogalmáról, 2.1. verzió, elfogadva 2021. július 7-én.
[19] A vonatkozó uniós szintű szabályozás a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról szóló 2015. november 5-i (EU) 2015/1998 bizottsági végrehajtási rendelet. Ez a rendelet azonban nem foglalkozik a hivatalos személyazonosító okmányoknak a repülőtéri ellenőrzőpontokon történő ellenőrzésével, így annak nemzeti szintű szabályozása a tagállamok mérlegelési jogkörébe tartozik.
[20] Ez azt jelenti, hogy jelenleg egyáltalán nem kerül sor ellenőrzésre, vagy csak a beszállókártya meglétét ellenőrzik. Például a dán, finn, norvég és svéd állampolgároknak a sajátjuktól eltérő skandináv országban való tartózkodásuk ideje alatt útlevéllel vagy tartózkodási engedéllyel való rendelkezés kötelezettsége alóli mentességéről szóló 1954. május 22-i jegyzőkönyv alapján 1954. július 1-jétől Norvégia, Dánia, Finnország és Svédország állampolgárai az ezen országok közötti utazásuk során mentesülnek azon kötelezettség alól, hogy útlevelet vagy más úti okmányt tartsanak maguknál.

utasok személyazonosságának ellenőrzésére vonatkozó jogi kötelezettségek előírása közvetlen hatással van az egyes repülőterek gyakorlatára.

18. Következésképpen ezekben a helyzetekben, amikor **nem szükséges az utasok személyazonosságának hivatalos személyazonosító okmánnyal történő igazolása, nem helyénvaló biometrikus ellenőrzést végezni, mert ez túlzott adatkezelést eredményezne, mivel a jelenlegi helyzethez képest további adatok kezelésével járna, és meghaladná az adott cél eléréséhez szükséges mértéket, megsértve ezzel az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontjában meghatározott adattakarékosság elvét**. Ezt a megfontolást a jelen vélemény 3.2 pontjában ismertetett valamennyi forgatókönyv vizsgálata során figyelembe kell venni.

2.2 Kulcsfogalmak

19. Az általános adatvédelmi rendelet 4. cikkének 14. pontja szerinti biometrikus adat kezelése[21] akkor valósul meg, ha a nyers adatok – például egy természetes személy testi, fiziológiai vagy viselkedési jellemzői – kezelése e jellemzők mérésével jár, mivel a biometrikus adatok ilyen mérések eredményei[22].

20. Az egyén arcáról készült felvétel (fénykép vagy videó) – ún. biometrikus **minta** – alapján leképezhető ezen arc sajátos jellemzőinek digitális megjelenítése (ún. „**sablon**”)[23]. Emellett a Testület emlékeztet arra, hogy „[a] biometrikus sablon biometrikus mintából leképezett egyedi jellemzők digitális reprezentációja, amely biometrikus adatbázisban tárolható[24]”, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását. Továbbá „[e]z a sablon elvileg minden személyre nézve egyedi és sajátos, és elvben az idő múlásával tartós[25]”. Jellemzően az egyén arcfelismeréssel történő azonosítását vagy hitelesítését célzó összehasonlítási folyamat során a beérkező biometrikus sablont tárolt objektumokkal hasonlítják össze az egyezés ellenőrzése vagy adatbázisban való megtalálása céljából[26].

[21] Lásd még az általános adatvédelmi rendelet (51), (52) és (53) preambulumbekezdését.
[22] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 74. bekezdés.
[23] Az Európai Adatvédelmi Testület 05/2022. sz. iránymutatásai az arcfelismerő technológia bűnüldözés területén történő alkalmazásáról, 2.0. változat, elfogadás időpontja: 2023. április 26. (a továbbiakban: **az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása**), 7. és 8. bekezdés.
[24] Ugyanott, 9. bekezdés.
[25] Ugyanott.
[26] Az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 10- 11. bekezdés; lásd még az ISO/IEC 2382–37, 2022–03 nemzetközi szabványt, elérhető a következő címen: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [legutóbbi hozzáférés: 2024. május 23.] (a továbbiakban: **ISO/IEC 2382–37**).

21. Az arcfelismerés két különböző funkciót – hitelesítés[27] és azonosítás[28] – tölthet be. Bár a két funkció elkülönül egymástól, mindkettő azonosított vagy azonosítható természetes személyre vonatkozó biometrikus adatok kezeléséhez kapcsolódik[29], ezért az általános adatvédelmi rendelet 9. cikke szerint a személyes adatok különleges kategóriái kezelésének minősül[30].

22. Konkrétan:

> A **hitelesítés** célja a biometrikus állítás összehasonlítás útján történő megerősítése. Ezt igazolásnak (egy az egyhez megfeleltetés) is nevezik.
>
> Az **azonosítás** célja, hogy a regisztrált biometrikus adatok adatbázisából egy adott egyénnek tulajdonítható azonosítókat kérdezzen le. Ezt egy a többhöz megfeleltetésnek (azonosításnak) is nevezik.

23. Az alkalmazott arcfelismerési technológiák mindkét esetben (tehát azonosítás és hitelesítés esetén is), az összehasonlítandó és a referencia-adatbázisban található sablonok közötti becsült egyezésen alapulnak. Ebből a szempontból ezek a technológiák probabilisztikusak: az összehasonlítás alapján nagyobb vagy kisebb valószínűséggel állapítható meg, hogy valóban a hitelesítendő vagy azonosítandó személyről van-e szó; ha ez a valószínűség meghalad egy bizonyos, a felhasználó vagy a rendszer fejlesztője által meghatározott egyezési küszöbértéket a rendszerben, akkor a rendszer feltételezi, hogy van azonosítandó vagy hitelesítendő egyezés[31].

[27] A Testület megjegyzi, hogy a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló európai parlamenti és tanácsi rendelet (a *Hivatalos Lapban* még nem tették közzé) 3. cikkének 36. pontja szerint is a biometrikus ellenőrzés „természetes személyek személyazonosságának automatizált, egy az egyhez ellenőrzése – ideértve a hitelesítést is – a biometrikus adataiknak a korábban megadott biometrikus adatokkal való összehasonlítása révén"; lásd az Európai Parlament 2024. március 13-i jogalkotási állásfoglalását a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Ugyanott; a mesterséges intelligenciáról szóló rendelet 3. cikkének 35. pontjában foglalt meghatározás szerint a biometrikus azonosítás „az ember fizikai, fiziológiai, viselkedési vagy pszichológiai humán jellemzőinek automatikus felismerése a természetes személy személyazonosságának megállapítása céljából, az említett egyén biometrikus adatainak az adatbázisban tárolt egyének biometrikus adataival való összehasonlítása révén".

[29] ISO/IEC 2382–37.

[30] Az általános adatvédelmi rendelet 4. cikkének 14. pontja és az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 12. bekezdés.

[31] Az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 11. bekezdés. Lásd még: ISO/IEC 2382–37.

3 A KÉRELEM ÉRDEMI VIZSGÁLATA

3.1 Általános észrevételek

24. Ez a szakasz a fenti 4. bekezdésben ismertetett kérdéseket elemzi. Ezzel összefüggésben a Testület az 1. kérdés esetében az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával, valamint 25. és 32. cikkével való összeegyeztethetőséget, a második kérdés esetében pedig az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével való összeegyeztethetőséget vizsgálja.

25. E célból a Testület négy különböző forgatókönyvet vizsgál[32], amelyek sajátos jellemzőit az alábbi 3.2. szakasz ismerteti.

26. Előzetes megjegyzésként a Testület emlékeztet arra, hogy a biometrikus adatok és különösen az arcfelismerő technológia használata fokozott kockázatokkal jár az érintettek jogaira és szabadságaira nézve. Elsősorban, a szóban forgó adatkezelés biometrikus adatokat érint, amelyek az általános adatvédelmi rendelet 9. cikke értelmében különleges védelmet élveznek. A biometrikus adatok ugyanis visszavonhatatlanul megváltoztatják a test és a személyazonosság közötti kapcsolatot, mivel az emberi test jellemzőit gép által leolvashatóvá és további felhasználásra alkalmassá teszik[33]. Emellett az arcfelismerő technológia használata hamis negatív azonosításhoz, torzításhoz és megkülönböztetéshez kapcsolódó kockázatokat idézhet elő[34], a biometrikus adatokkal való visszaélés lehetősége pedig súlyos következményekkel járhat az egyénekre nézve, például a személyazonossággal vagy a hasonmássággal való visszaélés esetén[35]. Említést érdemel továbbá, hogy ha az arcfelismerés távolról és az érintett aktív bevonása nélkül történik, előfordulhat, hogy az egyének még kevésbé tudnak az adatkezelésről és a kapcsolódó kockázatokról. Végezetül fontos hangsúlyozni, hogy a biometrikus adatok alapját képező jellemzők általában állandónak tekinthetők, és azokat visszavonhatatlannak kell tekinteni, különösen az arcfelismeréssel összefüggésben[36].

---

[32] A Testület által vizsgált négy forgatókönyv a kérelem I. mellékletében ismertetett használati eseteken alapul. A francia felügyeleti hatóság tisztázta, hogy a kérés I. mellékletében ismertetett használati esetek a megvalósítást szemléltető, egy adott forgatókönyvhöz tartozó példák.

[33] A 29. cikk szerinti munkacsoport 2012. április 27-én elfogadott 3/2012. sz. véleménye a biometrikus technológiák terén történt fejleményekről (a továbbiakban: **a 29. cikk szerinti munkacsoport 3/2012. sz. véleménye a biometrikus technológiákról**), WP193, 4. o. Említést érdemel, hogy a vélemény a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 1995. október 24-i 95/46/EK irányelvre (a továbbiakban: az adatvédelmi irányelv) hivatkozik. Az általános adatvédelmi rendelet az adatvédelmi irányelvhez képest a különleges adatkategóriák körét kiterjesztve ezek közé sorolja a biometrikus adatokat is (az általános adatvédelmi rendelet 9. cikke).

[34] Az Európa Tanács a személyes adatok kezelése vonatkozásában a természetes személyek védelmére vonatkozó egyezménnyel foglalkozó konzultatív bizottságának iránymutatásai, 2021. június, 15. o.; lásd még: az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 27. bekezdés.

[35] Lásd még a 29. cikk szerinti munkacsoport biometrikus technológiákról szóló 3/2012. sz. véleményét, 29. o.

[36] Az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 104. bekezdés.

27. A fentiek figyelembevételével, emiatt az ilyen technológiák használata előtt – még ha azok különösen hatékonynak tekinthetők is – az adatkezelőknek fel kell mérniük az érintettek alapvető jogaira és szabadságaira gyakorolt hatást, és meg kell vizsgálniuk, hogy az adatkezelés törvényes célja elérhető-e kevésbé intruzív eszközökkel[37].

28. A Testület emlékeztet továbbá arra, hogy a személyes adatok védelméhez való jog nem abszolút jog, és azt az arányosság elvével összhangban egyensúlyba kell hozni a Charta által védett egyéb alapvető jogokkal[38].

29. Az általános adatvédelmi rendelet 25. cikkének (1) bekezdése az általános adatvédelmi rendelet 5. cikkében felsorolt „adatvédelmi elvekre" hivatkozva[39] azok beépített, „hatékony megvalósítását" írja elő[40]. Ez kifejezetten magában foglalja az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja szerinti adattakarékosság elvét[41], amely előírja, hogy a személyes adatoknak „az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk[42]" – ebben az arányosság elve nyer megfogalmazást. Emellett az általános adatvédelmi rendelet 25. cikkének (2) bekezdése az „alapértelmezett adattakarékosság" kötelezettség dimenzióit

[37] Az általános adatvédelmi rendelet (39) preambulumbekezdése. Lásd még az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatásának 73. bekezdését.

[38] Az általános adatvédelmi rendelet (4) preambulumbekezdése. Lásd még e tekintetben: a Bíróság C-439/19. sz., Latvijas Republikas Saeima ügyben hozott 2021. június 22-i ítélete, ECLI:EU:C:2021:504 (a továbbiakban: a C-439/19. sz., Latvijas Republikas Saeima ügyben hozott ítélet), 98., 110. és 113. pont. Ezenkívül az arányosság elve mint az uniós jog általános elve megköveteli, hogy az uniós jogi aktusok által végrehajtott intézkedések alkalmasak legyenek a kitűzött cél megvalósítására, és ne lépjék túl az annak eléréséhez szükséges mértéket – lásd a Bíróság C-92/09 és C-93/09. sz., Volker és Markus Schecke és Eifert ügyben hozott 2010. november 9-i ítéletének (ECLI:EU:C:2010:662, a továbbiakban: a C–92/09 és C–93/09. sz., Volker és Markus Schecke és Eifert ügyben hozott ítélete) 74. pontját, valamint az ott hivatkozott ítélkezési gyakorlatot.

[39] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0. változat, elfogadás időpontja: 2020. október 20. (a továbbiakban: **az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a beépített és alapértelmezett adatvédelemről**), 11. bekezdés.

[40] Az általános adatvédelmi rendelet 25. cikkének (1) bekezdése a következőképpen rendelkezik: „Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába." Lásd az Európai Adatvédelmi Testület 4/2019. sz. iránymutatását a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 13. bekezdés.

[41] Ennek megfelelően az általános adatvédelmi rendelet (39) preambulumbekezdése kimondja, hogy személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.

[42] A C-439/19. sz., Latvijas Republikas Saeima ügyben hozott ítélet 98. pontja; a Bíróság C-708/18. sz., Asociaţia de Proprietari bloc M5A-ScaraA ügyben hozott 2019. december 11-i ítéletének (ECLI:EU:C:2019:1064, a továbbiakban: a C-708/18. sz., M5A-ScaraA ügyben hozott ítélet) 48. pontja.

akként határozza meg, hogy az kiterjed a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre[43].

30. Az általános adatvédelmi rendelet 25. cikke azonban nem írja elő az adatkezelők számára konkrét technikai és szervezési intézkedések végrehajtását, hanem azt írja elő, hogy a választott intézkedéseknek és biztosítékoknak a konkrét körülményekhez, valamint az adatkezelés által az érintett jogaira és szabadságaira jelentett kockázatokhoz kell igazodniuk[44]. Ugyanígy az általános adatvédelmi rendeletnek az adatkezelés biztonságáról szóló 32. cikke előírja az adatkezelők és az adatfeldolgozók számára, hogy megfelelő technikai és szervezési intézkedéseket hajtsanak végre, amelyek garantálják a természetes személyek jogaira és szabadságaira jelentett kockázat mértékének megfelelő szintű adatbiztonságot.

31. Fontos, hogy még ha az utasok kifejezetten hozzájárulnának is biometrikus adataik felhasználásához a repülőterek utasforgalmának egyszerűsítése érdekében, az általános adatvédelmi rendeletben a szükségesség és arányosság tekintetében rögzített adatkezelési elvek továbbra is alkalmazandók, és azokat be kell tartani[45].

32. A **szükségesség elvét** illetően a Testület azt mérlegeli, hogy a tervezett adatkezelés szükséges-e a kitűzött cél eléréséhez, és hogy ugyanaz a cél azonos hatékonyság mellett elérhető-e más, az érintettek alapvető jogait és szabadságait kevésbé csorbító eszközökkel[46]. Az **arányosság elvét** illetően a Testület azt értékeli, hogy az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás arányos-e a várható előnyökkel. Ha az előny viszonylag csekély, a hatás nem feltétlenül arányos[47].

33. Mindenesetre, még ha a Testület úgy is ítéli meg, hogy az alábbiakban vizsgált forgatókönyvek valamelyike megfelelhet az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjában, valamint 25. és 32. cikkében foglalt követelményeknek, ezt minden esetben az adatkezelőnek kell bizonyítania tényszerű elemekkel. A bizonyítás során alternatív forgatókönyveket is figyelembe kell vennie.

3.2 Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével való összeegyeztethetőségről

[43] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 48. bekezdés.
[44] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 14. bekezdés.
[45] Az Európai Adatvédelmi Testület 5/2020 sz. iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, 5. bekezdés.
[46] A C-439/19. sz., Latvijas Republikas Saeima ügyben hozott ítélet 110. és 113. pontja; az Európai Unió Bíróságának (nagytanács) a C-252/21. sz.,Meta kontra Bundeskartellamt ügyben hozott 2023. július 4-i ítélete (ECLI:EU:C:2023:537), 108. pont.
[47] A C-708/18. sz., M5A-ScaraA ügyben hozott ítélet 52–56. pontja; a C–92/09 és C–93/09. sz., Volker és Markus Schecke és Eifert ügyben hozott ítélet 87. pontja; a C-439/19. sz., Latvijas Republikas Saeima ügyben hozott ítélet 98., 110., 113. pontja. Lásd még a 29. cikk szerinti munkacsoport biometrikus technológiákról szóló 3/2012. sz. véleményét, 8. o.

3.2.1 1. forgatókönyv: a regisztrált biometrikus sablon tárolása kizárólag az egyénnél, hitelesítés céljából

34. Ez a szakasz azt vizsgálja, hogy összeegyeztethető-e az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával, valamint 25. és 32. cikkével, ha az utasok biometrikus sablonját kizárólag az egyénnél, például annak személyes eszközén[48] és kizárólagos ellenőrzése alatt[49] tárolják hitelesítés céljából[50] (a továbbiakban: **1. forgatókönyv**). Ez a szakasz az 1. forgatókönyvre vonatkozó megfelelő biztosítékokat is vizsgálja az általános adatvédelmi rendelet 25. és 32. cikkének fényében.

A forgatókönyv ismertetése

35. Az 1. forgatókönyv szerint az adatkezeléshez hozzájáruló egyes utasok regisztrált biometrikus sablonját kizárólag náluk, például a kizárólagos ellenőrzésük alatt lévő (személyes) eszközökön tárolják. Az utasokat a meghatározott repülőtéri ellenőrzőpontokon való áthaladáskor hitelesítik (1:1 összehasonlítással).

36. A regisztrációt a repülőtér-üzembentartó végzi vagy távolról a saját alkalmazásával[51] vagy olyan repülőtéri terminálokon keresztül, amelyek a személyazonosság tekintetében megfelelő szintű bizonyosságot nyújtanak (pl. az eIDAS[52] szerint). A regisztráció az utas eszközén az adatkezeléshez szükséges biometrikus sablon és azonosító adatok[53] rögzítéséből áll. A regisztráció egyszeri, és meghatározott érvényességi időszakra szól, amely például az utas útlevelének érvényességi idejéhez igazodhat. A regisztrációs eljárást követően a repülőtér-üzembentartó sem az utasok azonosító adatait, sem biometrikus adataikat nem őrzi meg.

37. Ami a tárolást illeti, az utas azonosító adatait és biometrikus sablonját helyben tárolják az egyes utasok eszközén (pl. a repülőtér-üzembentartó mobilalkalmazásában vagy digitális személyiadat-tárca alkalmazásban). Az eszköz ezt követően használható az utasok azonosító adatai és biometrikus sablonja továbbítására vagy lekérdezésére, akár a járatinformációkra és/vagy a beszállókártyára is kiterjedően. Ezt az információt például egy kizárólag a repülőtér-üzembentartó birtokában lévő kulccsal titkosítják – ez akár QR-kód formájában kódolható, amely papírra nyomtatható, vagy az utas eszközének képernyőjén is megjeleníthető. Ebben az esetben az utas ezt a QR-kódot a repülőtéren

[48] Alternatív megoldásként az egyén kinyomtathatja és papíron tárolhatja a biometrikus sablonját.
[49] Ez nem érinti az adatkezelő adatkezeléssel kapcsolatos általános felelősségét.
[50] A kérelem I. mellékletében szereplő 1. gyakorlati eset példáján keresztül.
[51] Az Európai Adatvédelmi Testület megjegyzi, hogy a jövőben a regisztráció alternatív módjait is elő lehetne irányozni, és azt akár külön repülőtér-üzembentartói alkalmazás nélkül, például a felhasználó digitális személyiadat-tárcájával való interakció révén is el lehetne végezni.
[52] Elektronikus azonosítási és bizalmi szolgáltatási keret (a továbbiakban: **eIDAS**), amelynek alapja a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról szóló, 2024. április 11-i (EU) 2024/1183 európai parlamenti és tanácsi rendelet.
[53] A jelen vélemény alkalmazásában az azonosító adatok olyan adatokat (családi nevet, utónevet, születési időt stb.) jelölnek, amelyek helytállósága személyazonosító okmány vagy útlevél alapján igazolást nyert.

egy QR-szkennerrel és kamerával felszerelt, erre a célra kialakított ellenőrzőegységnél (pod) mutatná fel.

38. Ami a biztonságot illeti, a megfeleltetés során a QR-kódokat az azok dekódolására kizárólagosan képes repülőtér-üzembentartó birtokában lévő kulccsal dekódolják. Az utasok biometrikus adatait csak nagyon rövid ideig őrzik meg, majd a megfeleltetést követően törlik. Meg kell jegyezni, hogy a tárolásra vonatkozó biztonsági intézkedések részben az utas eszközének biztonságától függenek.

Az Európai Adatvédelmi Testület értékelése

39. Az 1. forgatókönyv olyan műszaki és szervezeti intézkedéseket ismertet, amelyek célja az érintetteket érintő kockázatoknak megfelelő biztonsági szint biztosítása az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjában és 32. cikkében előírtak szerint. Az utasokat a meghatározott repülőtéri ellenőrzőpontokon való áthaladáskor hitelesítik (1:1 összehasonlítással). Ennél a forgatókönyvnél a fő megfeleltetési művelet ellenőrzött környezetben zajlik[54] az utasok aktív részvételével, akik ennélfogva nagyobb ellenőrzéssel bírnak adataik felett. Különösen, csak azokat az utasokat ellenőriznék, akik hozzájárultak az adatkezeléshez, és mivel az ellenőrzésük külön erre a célra kialakított ellenőrzőegységeknél történne, az adatkezeléshez hozzá nem járuló többi utas biometrikus adatait nem gyűjtenék. Emellett a hozzájárulásukat adó utasoknak lehetőségük van arra, hogy az adatok eszközükről való törlésével bármikor leállítsák az adatkezelést.

40. A kizárólag az egyénnél – például a magánál tartott, kizárólagos ellenőrzése alatt lévő (személyes) eszközén – tárolt biometrikus sablonon alapuló arcfelismerés meghatározott ellenőrzőpontokon, külön interfészen keresztüli hitelesítésre történő alkalmazása bizonyos feltételek mellett kevesebb kockázatot jelent a központosított adatbázisban tárolt biometrikus adatok használatához képest[55]. A lokalizált tárolás – amennyiben ahhoz megfelelő biztosítékok társulnak[56] – a központosított tároláshoz képest csökkenti a személyes adatok megsértésének súlyosságát az érintett személyek száma tekintetében, és biztosítja, hogy a biometrikus sablonhoz való hozzáférés az érintett aktív bevonásával történjen.

41. Ezenkívül a megfeleltetés helyben, a repülőtéren is elvégezhető, a – például a QR-kódban foglalt – biometrikus sablon és az ellenőrzőegység kamerája által rögzített biometrikus minta alapján kiszámított sablon kimenetének összehasonlításával. A célzott ellenőrzést végző adatkezelő (amely lehet repülőtér-üzembentartó vagy légitársaság attól függően, hogy az ellenőrzésre a repülőtéri biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor és/vagy a várókba történő belépéskor kerül-e sor) csak a megfeleltetés eredményét ismeri meg és használja fel. Emellett az, hogy

[54] „Ellenőrizetlen környezetről" van szó, ha a személyazonosítás céljára történő használatra az érintettek aktív közreműködése nélkül kerül sor, ekkor a megfigyelési területre belépő minden egyes arc sablonját összehasonlítják az adatbázisban tárolt, a populáció széles keresztmetszetéből származó sablonokkal; lásd: az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 17. bekezdés.

[55] Az Európai Adatvédelmi Testület a bűnüldözés során alkalmazott arcfelismerésről szóló 5/2022. sz. iránymutatása, 17. bekezdés.

[56] Ezek tárgyalását lásd alább a 46. ponttól.

a megfeleltetéshez szükséges információkat (pl. a QR-kódot) az egyénnek kell megadnia, második faktorként szolgál[57], és ezáltal erősíti a hitelesítés biztonságát.

42. Ami az általános adatvédelmi rendelet 25. cikkével való összeegyeztethetőséget illeti, és különösen az adattakarékosság követelményének való megfelelés érdekében biztosítani kell, hogy az adatkezelés megfeleljen a szükségesség elvének. Az 1. forgatókönyv esetében a választott intézkedések a kitűzött céllal (az utasforgalom egyszerűsítésével) összefüggésben akkor tekinthetők a szükségesség elvének megfelelőnek, ha az adatkezelés körülményeitől függően az adatkezelő bizonyítani tudja, hogy nincsenek olyan kevésbé intruzív alternatív megoldások, amelyekkel ugyanaz a cél hatékonyan elérhető. Például az adatkezelő bizonyítani tudja, hogy még ha az utasoknak be is kellene mutatniuk eszközüket, az 1. forgatókönyv felgyorsítja az ellenőrzési folyamatot a jelenlegi helyzethez képest, ahol emberi ellenőrzés keretében vizsgálják, hogy a beszállókártyán szereplő név egyezik-e az utas személyazonosító okmányával[58]. Ez ugyanis nem állapítható meg akkor, ha jelenleg nem végeznek ellenőrzéseket az utasok személyazonosságának a hivatalos személyazonosító okmányuk alapján történő igazolására (lásd e tekintetben a fenti 18. pontot).

43. Ezenkívül a biometrikus sablonokat a repülőtér-üzembentartó nem őrzi meg a nyilvántartásba vételt követően, a biometrikus adatoknak az ellenőrzést végző adatkezelőnél való megőrzési ideje pedig nagyon rövid, mivel ezeket az adatokat a megfeleltetés befejeztével törlik. Ennélfogva úgy tűnik, hogy az 1. forgatókönyvben választott intézkedések korlátozzák a személyes adatok kezelésének mértékét és tárolási időtartamát.

44. Az arányosság elvét illetően az adatkezelés intruzív jellegét ellensúlyozhatja az utasok aktív részvétele, mivel biometrikus adataik tárolása kizárólag náluk történne. Ezen túlmenően, figyelembe véve az előzőekben ismertetett intézkedéseket, továbbá feltételezve, hogy az adatkezelő a szóban forgó konkrét adatkezelés által megkövetelt megfelelő biztosítékokat érvényesíti, a megfelelő intézkedések végrehajtása garantálhatja a kockázat mértékének megfelelő szintű biztonságot. Ebben az esetben az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás arányosnak tekinthető a várható haszonnal.

45. Ezért a fentiekre tekintettel az 1.1. kérdésre válaszolva a Testület arra a következtetésre jut, hogy az adatkezelés – **megfelelő biztosítékok mellett – elvben összeegyeztethetőnek tekinthető az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával, valamint 25. és 32. cikkével**.

Megfelelő biztosítékok

46. Ilyen típusú forgatókönyv esetén az 1.2. kérdésre válaszolva a Testület legalább az alábbi biztosítékok érvényesítését tartja szükségesnek. *A jelen véleményben leírtaktól eltérő biztosítékok alkalmasak lehetnek ugyanazon biztonsági és adatvédelmi célok elérésére, emellett jogszerűek is lehetnek, amennyiben biztosítják az alkalmazandó jogi keretnek való megfelelést*.

[57] Ez például csökkenti a személyazonossággal való visszaélés kockázatát. Lásd még az alábbi C.1.2. biztosítékot.
[58] Elmondható továbbá, hogy a biometrikus ellenőrzésnél kisebb valószínűséggel fordulnak elő hibák az emberi ellenőrzéshez képest.

47. Megjegyzés: *az alábbiak általános, nem teljes körű áttekintést adnak olyan megfelelő biztosítékokról, amelyeket az adatkezelőnek az 1. forgatókönyvhöz hasonló megoldás alkalmazása esetén kell érvényesítenie. Az általános adatvédelmi rendelet 25. és 32. cikke szerinti megfelelőségük esettől függően állapítható meg. Valamennyi adatkezelőnek gondoskodnia kell saját adatvédelmi hatásvizsgálat elvégzéséről[59], és konkrét megoldásaik további, ebben a véleményben nem szereplő intézkedéseket tehetnek szükségessé*.

A. Általános szempontok

A.1. Adatkezelési hatásvizsgálat

A.1.1. Az általános adatvédelmi rendelet 35. cikkének követelményeivel összhangban adatvédelmi hatásvizsgálatot kell végezni minden olyan esetben, amikor az adatkezelő olyan új adatkezelési műveletet tervez, amely valószínűleg magas kockázattal jár. Ez a helyzet valószínű az 1. forgatókönyv esetében, amely a biometrikus adatok nagy léptékű feldolgozásával jár[60]. A korai tervezési szakaszban értékelni kell az arcfelismerő rendszer bevezetésének megfelelőségét, beleértve annak szükségességét és arányosságát a kitűzött célokhoz képest[61], és azt a termékfejlesztés teljes életciklusa során felül kell vizsgálni.

A.1.2. Amennyiben az adatkezelő által a kockázat csökkentése érdekében hozott intézkedések ellenére az adatkezelés továbbra is magas kockázattal jár, konzultálni kell az érintett felügyeleti hatósággal[62].

A.2. Az érintettek jogai és az adatkezelők által érvényesíthető biztosítékok

A.2.1. A hamis negatív azonosítási esetek kezelését szolgáló biztosítékok. Csökkenteni kell az életkor, a nem és a faj szerinti torzulások elfogultság kockázatát, ennek érdekében „rendszeresen értékelni kell, hogy az algoritmusok a célnak megfelelően működnek-e, a feltárt torzulások mérséklése érdekében az algoritmusokat módosítani kell, és biztosítani kell, hogy az adatkezelés tisztességes legyen[63]”. Ez megvalósulhat például emberi felügyelet és beavatkozás révén, amelynek célja az esetleges torzulások enyhítése, valamint utasok stigmatizálásának vagy a róluk való profilalkotásnak az elkerülése.

[59] Az általános adatvédelmi rendelet 35. cikke.
[60] Az általános adatvédelmi rendelet 35. cikkének (3) bekezdése; a 29. cikk szerinti munkacsoport 2017. október 13-án elfogadott iránymutatása az adatvédelmi hatásvizsgálat elvégzéséről és annak megállapításáról, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal” jár-e, WP248 rev.01, az Európai Adatvédelmi Testület által jóváhagyva.
[61] Az általános adatvédelmi rendelet 35. cikke (7) bekezdésének b) pontja.
[62] Az általános adatvédelmi rendelet 36. cikkének (1) bekezdése.
[63] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 60. lábjegyzet, 70. bekezdés.

A.2.2. Biztosítani kell, hogy a személyes adatok kezelése minden esetben átlátható legyen, és az egyének tisztában legyenek azzal, hogy adataikat hogyan kezelik és dolgozzák fel az egyes adatkezelési műveletek során[64].

A.2.3. Biztosítani kell a célhoz kötöttség elvének való megfelelést célzó intézkedéseket annak érdekében, hogy az adatokat ne használják fel más célokra, például biztonsági vagy képzési célokra.

A.2.4. Megfelelő intézkedésekkel (például a mélységélesség és képrögzítési felbontás olyan megválasztásával, amellyel elkerülhető a háttérben vagy a környéken tartózkodó más utasok képmásának rögzítése, vagy az arcfelismerés céljára egyértelműen megjelölt sorok kialakításával) biztosítani kell, hogy ne készüljön fénykép vagy videó – akkor sem, ha azt nem rögzítik és nem dolgozzák fel – olyan egyénről, aki nem járult hozzá az arcfelismeréshez.

A.2.5. Amennyiben az arcfelismeréshez hozzájáruló és ahhoz hozzá nem járuló utasok ugyanazokat az ellenőrzőegységeket használhatják, vagy ha a rendszer használaton kívüli állapotában az arcfelismeréshez hozzá nem járuló utasok jelenhetnek meg a látómezőben, a fénykép vagy videó rögzítése csak a hozzájárulását adó utas határozott jelzésére kezdhető meg.

A.2.6. Az érintett számára lehetővé kell tenni, hogy bármikor törölje a kizárólag nála, mobilalkalmazásban vagy digitálisadat-tárcában tárolt adatokat (biometrikus sablont[65])[66].

A.2.7. Gondoskodni kell megvalósítható alternatívákról vagy tartalékmegoldásokról (azon utasok számára, akik nem járulnak hozzá biometrikus adataik felhasználásához, vagy nem tudják használni az ilyen megoldásokat, vagy hibás elutasítást szenvednek el), hogy azok az utasok se szenvedjenek hátrányt, akik nem járulnak hozzá a szóban forgó adatkezeléshez[67].

A.2.8. Egy alkalmazás használata esetén azt gondosan meg kell tervezni és konfigurálni kell annak érdekében, hogy ne gyűjtsön szükségtelen adatokat, és elkerülhető legyen az adatokat más célokra gyűjtő, harmadik féltől származó szoftverfejlesztő készletek (SDK) használata.

A.3. Elszámoltathatóság

[64] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 68. bekezdés; az általános adatvédelmi rendelet (7) preambulumbekezdése.
[65] Az 1. forgatókönyv szerinti biztosítékoknál a biometrikus sablonra való hivatkozások a 2. forgatókönyv szerinti kulcsra, illetve titkos adatra való hivatkozásoknak felelnek meg.
[66] Ez a biztosíték csak az 1. forgatókönyvre vonatkozik.
[67] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 86. bekezdés.

A.3.1. Értékelni kell az olyan magatartási kódexek vagy tanúsítási mechanizmusok meglétét, amelyek elősegíthetik az általános adatvédelmi rendelet 32. cikkében az adatkezelés biztonságára vonatkozóan előírtaknak való megfelelés igazolását[68]. Az adatkezelőnek az adott adatkezelési folyamattal összefüggésben kell ellenőriznie az intézkedések megfelelőségét. Az adatkezelők különböző kategóriáit képviselő egyesületek és egyéb szervek által elismert szabványok[69], bevált gyakorlatok és magatartási kódexek segítséget nyújthatnak a megfelelő intézkedések meghatározásához.

A.3.2. Biztosítani kell az alapvető biztonsági ellenőrzések elvégzését a felhasználók eszközén a regisztrációs szakasz lehetővé tétele érdekében, annak ellenére, hogy adatai védelmében az utas is szerephez jut, mivel azokat az eszközén tárolja. Az ilyen technikai ellenőrzésekre és kontrollokra az alábbi C.2. szakasz („Infrastruktúra és hálózat") mutat be példákat.

B. Szervezeti szempontok:

B.1. Szabályozás és megfelelés

B.1.1. Gondoskodni kell belső hozzáférési kontrollok[70] és az adminisztrátorokra vonatkozó szabályok meglétéről.

B.1.2. Amennyiben az arcfelismerő szolgáltatást az adatkezelésben részt vevő felek egyike anélkül is nyújthatja, hogy a többi érintett félnek személyazonosító vagy biometrikus adatokat vagy mindkét adatfajtát kezelnie kellene, meg kell tiltani ezen adatoknak a többi érintett félnek történő továbbítását. Például egy légitársaságnak, amely a közös repülőtéri infrastruktúrát veszi igénybe, technikailag még akkor sem szükséges hozzáférnie a biometrikus adatokhoz, ha az adott légitársaság az általános adatvédelmi rendelet szerinti adatkezelés adatkezelőjeként jár el.

B.1.3. A titkosításra és a rejtjelkulcs-kezelésre vonatkozó szabályzatot kell kidolgozni[71] többek között az azonosító és biometrikus adatok kezelésére kiterjedően.

[68] Az általános adatvédelmi rendelet 32. cikkének (3) bekezdése; az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 10. bekezdés.
[69] Lásd például: ISO/IEC 2382–37.
[70] Az Európai Adatvédelmi Testület 2020. április 21-én elfogadott 04/2020 sz. iránymutatása a Covid19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról (a továbbiakban: **az Európai Adatvédelmi Testület 4/2020 sz. iránymutatása a helymeghatározó adatokról és a kontaktkövető eszközökről**), SEC-10, 16. o.
[71] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 89. bekezdés.

B.1.4. Biztosítani kell az általános adatvédelmi rendelet V. fejezetének való megfelelést. Például a megfelelő adattovábbítások biztosításával, ha az adatkezelő a regisztrációs folyamat során harmadik országban található távoli szolgáltatást vesz igénybe.

B.1.5. Adatfeldolgozó igénybevétele esetén gondoskodni kell az általános adatvédelmi rendelet 28. cikkének (3) bekezdése szerinti adatfeldolgozói megállapodás meglétéről[72].

B.1.6. Biztosítani kell az emberi felügyelet és beavatkozás kezelésére szolgáló eljárások meglétét, különösen a hibás elutasítással kapcsolatos, valamint a technikai vagy használhatósági problémák elhárítása céljából.

B.2. Képzés és tesztelés

B.2.1. Biztosítani kell a személyzet megfelelő képzését.

B.2.2. Gondoskodni kell „az adatkezelés biztonságát szolgáló technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás" bevezetéséről[73].

B.2.3. Eljárást kell bevezetni annak biztosítására, hogy az utas biometrikus sablonjának[74] hitelesítés céljából történő kezelése technikailag hatékony és kellően pontos legyen.

B.2.4. Biztosítani kell, hogy mind a regisztrációkor, mind az ellenőrzőponton vett biometrikus minták megfelelő minőségűek legyenek a megbízható biometrikus adatkezelés elvégzéséhez.

C. Műszaki szempontok:

C.1. Hozzáférés

C.1.1. Biztosítékokat kell érvényesíteni a regisztrációs szakaszban annak biztosítása érdekében, hogy a regisztrációs folyamatot ellenőrzött személyazonossággal lehessen előkészíteni. Például lépéseket lehet tenni a felhasználói személyazonosság többfaktoros hitelesítésének megerősítésére, az alkalmazás aktiválására szolgáló, jelszóval védett egyszer használható linkektől az eszközök blokkolását lokálisan megszüntető mechanizmusokig.

[72] Az általános adatvédelmi rendelet 28. cikkének (3) bekezdése.
[73] Az általános adatvédelmi rendelet 32. cikke (1) bekezdésének d) pontja.
[74] Az 1. forgatókönyv szerinti biztosítékoknál a biometrikus sablonra való hivatkozások a 2. forgatókönyv szerinti kulcsra, illetve titkos adatra való hivatkozásoknak felelnek meg.

C.1.2. Biztosítékokat kell érvényesíteni a hamis pozitív azonosítások, a megjelenítési támadások és a csalásmegelőzés kezelésére[75].

C.1.3. Le kell tiltani a személyazonossági- és biometrikus adatokhoz való külső hozzáférést[76].

C.1.4. Biztosítani kell, hogy az adatkezelés a regisztrációs, továbbítási és megfeleltetési szakaszban helyi szinten történjen. A megfeleltetési pontnak a lehető legközelebb kell lennie az egyén eszközéhez. A sablon egyéni eszközön belüli egyeztetéséhez szükség lehet a repülőtéren kívüli szolgáltatókkal való interakcióra és nyilvános hálózati erőforrások felhasználására, ekkor hátrányként jelentkezhet a rendelkezésre állásra gyakorolt hatás, valamint a sablon külső szereplők körében való terjesztése.

C.1.5. A felhasználót új járat hozzáadásakor és új titkosított QR-kód létrehozásakor hitelesíteni kell.

C.1.6. Intézkedéseket kell végrehajtani annak az esetleges helyzetnek a kezelésére, amikor az utas elveszíti QR-kódjához való hozzáférését.

C.2. Infrastruktúra és hálózat

C.2.1. Az operációs rendszerre (OS) vonatkozó feltételeket naprakészen kell tartani, továbbá lehetővé kell tenni a hitelesítést az alkalmazás vagy a digitálisadat-tárca működéséhez szükséges eszközhöz való hozzáférésre vonatkozóan; ennek körében az azonosító és biometrikus adatokat automatikusan törölni kell, amennyiben az operációs rendszer elavult és biztonsági kockázatot jelent.

C.2.2. Üzem közben az egyeztető (ellenőrző) egységek leválasztása a hálózatról, valamint minden egyéb szükséges biztonsági intézkedés meghozatala.

C.2.3. A biometrikus megfeleltetést az utas eszközén vagy az ellenőrző egységen kell elvégezni (pereminformatika).

C.2.4. Az utasok egyéni eszközeit érintő biztonsági sebezhetőségek kezelésére szolgáló megoldásokat kell alkalmazni, beleértve (minimálisan) az inaktív biometrikus és azonosító adatok titkosítását.

C.2.5. Biztonságos tárolás használata annak érdekében, hogy (legalább) a biometrikus adatok tárolása kizárólag a felhasználónál történjen[77], például okostelefonon kialakított biztonságos enklávé útján.

[75] Az ENISA 2022. januári jelentése a digitális személyazonosságról: Az önállóan kezelt személyazonosság (SSI) koncepciójának bizalomépítési célú felhasználása.
[76] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 89. bekezdés.
[77] Az 1. forgatókönyv szerinti biztosítékoknál a biometrikus sablonra való hivatkozások a 2. forgatókönyv szerinti kulcsra, illetve titkos adatra való hivatkozásoknak felelnek meg.

C.2.6. A helyiségek, többek között a repülőtéri biometrikus terminál fizikai biztonságát garantáló biztosítékokat kell érvényesíteni. Garantálni kell az architektúra azon elemeinek (pl. számítás, adatáramlás, átmeneti vagy hosszú távú tárolás) magas szintű biztonságát, amelyek azonosító és biometrikus adatok kezelését végzik.

C.3. Adatbiztonság és -kezelés a felhasználó személyazonosságának ellenőrzésekor

C.3.1. Az adatokat a továbbítás és tárolás során legalább három különböző kategóriában, például azonosító, biometrikus és járatadatok szerint kell elkülöníteni[78]. Biztosítani kell az adatok továbbítás és tárolás közötti megfelelő titkosítását.

C.3.2. Olyan technikai intézkedéseket kell bevezetni, amelyek biztosítják, hogy az egyes ellenőrzőpontokon csak az ott jogszerűen kezelhető adatok kezelésére és ellenőrzésére kerüljön sor.

C.3.3. Biztosítani kell az adattörlés eredményességét[79] biztonságos (például az elsődleges memóriára, a gyorsítótárra, az esetleges biztonsági másolatokra is kiterjedő) törlési eljárás révén, továbbá értékelni kell, hogy az adattörlés automatizálása mikor indokolt. Az adattárolási időtartamokat szigorúan érvényesíteni kell automatikus rutinok révén, anélkül, hogy az egyén részéről kiegészítő intézkedésre lenne szükség[80].

C.3.4. Biztosítani kell az adatok hitelességét és integritását (például aláírással)[81].

C.3.5. Az utasok biometrikus adatai csak nagyon rövid ideig őrizhetők meg a regisztrációs ponton és az ellenőrzőponton, és azokat az utas ellenőrzőponton történő áthaladását követően azonnal törölni kell.

C.3.6. A regisztrációhoz használt alkalmazás esetén annak fejlesztése során a mobilalkalmazások biztonságára vonatkozó biztonsági szabványokat kell alkalmazni, a biztonsági teszteket pedig harmadik félnek kell elvégeznie.

C.3.7. A biometrikus utasadatok integritásának és bizalmas jellegének megőrzése érdekében gondoskodni kell arról, hogy a repülőtéren a regisztrációs szakaszhoz kapcsolódó biztonsági intézkedések legyenek érvényben. Ha például a QR-kód nyomtatását a kioszk végzi, akkor ott a QR-kód nem jeleníthető meg, hogy arról rosszindulatú szereplő ne készíthessen képet. A

[78] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 89. bekezdés.
[79] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 89. bekezdés.
[80] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 82. bekezdés.
[81] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 89. bekezdés.

rövid távolságú adattovábbítást a felhasználó aktív részvételével, a közelséget biztosító csatornán keresztül kell végrehajtani.

C.3.8. A kizárólag az egyénnél tárolt adatokat[82] biztonságos tárolóban kell tárolni az adott egyén eszközén, és az eszköz operációs rendszereit érintő esetleges sebezhetőségeknél alkalmazni kell a megfelelő biztonsági javításokat. Nyomtatott QR-kód esetén az egyént tájékoztatni kell a kódban foglalt adatok különlegesen érzékeny jellegéről és a kóddal végezhető műveletekről.

C.3.9. Biztosítani kell, hogy a regisztrációra megfelelő távoli személyazonosság-igazolási technikák mentén kerüljön sor[83].

3.2.2 2. forgatókönyv: a regisztrált biometrikus sablon központosított, a repülőtéren titkosított formában történő tárolása hitelesítés céljából, valamint a kizárólag az utasnál lévő kulccsal vagy titkos adattal való társítása

48. Ez a szakasz azt vizsgálja, hogy az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével összeegyeztethető-e az utasok regisztrált biometrikus sablonjának központosított, titkosított formában történő tárolása hitelesítés céljából, valamint a kizárólag az utasnál lévő kulccsal vagy titkos adattal való társítása[84] (a továbbiakban: **2. forgatókönyv**). Ez a szakasz a 2. forgatókönyvre vonatkozó megfelelő biztosítékokat is vizsgálja az általános adatvédelmi rendelet 25. és 32. cikkének fényében.

A forgatókönyv ismertetése

49. A 2. forgatókönyv szerint a regisztrációra csak egyszer – távolról, a személyazonosság tekintetében megfelelő szintű bizonyosság mellett (pl. az eIDAS szerint) vagy a repülőtéri terminálokon – kerül sor, és az meghatározott időtartamra érvényes, amely lehet például az utolsó úttól számított egy év, vagy az útlevél érvényességi ideje. A regisztrációt a repülőtér-üzembentartó irányítja; a művelet kulccsal vagy titkos adattal titkosított azonosító és biometrikus adatok generálásából áll.

50. Az adatbázist a repülőtér-üzemeltető ellenőrzése alatt, a repülőtér területén tárolják. Az egyedi titkosítási kulcsokat vagy titkos adatokat kizárólag az egyén eszközén tárolják (például a repülőtér-üzembentartó mobilalkalmazásában). Az alkalmazás a kulcsot vagy titkos adatot tartalmazó QR-kódot

[82] Az 1. forgatókönyv szerinti biztosítékoknál a biometrikus sablonra való hivatkozások a 2. forgatókönyv szerinti kulcsra, illetve titkos adatra való hivatkozásoknak felelnek meg.
[83] Lásd az ENISA „Jelentés a távoli személyazonosság-igazolásról: A személyazonosság távolról történő igazolására szolgáló módszerek elemzése” című jelentését (2021. március).
[84] A kérelem I. mellékletében szereplő 2. gyakorlati eset példáján keresztül.

hozhat létre, amely papírra nyomtatható, vagy megjeleníthető az eszköz kijelzőjén[85]. Emellett a titkosítás második rétegéről[86] a repülőtér-üzembentartó gondoskodik az általa ellenőrzött kulcsokkal.

51. Az utasokat a meghatározott repülőtéri ellenőrzőpontokon való áthaladáskor hitelesítik (1:1 összehasonlítással). Azok az utasok, akik úgy döntenek, hogy áthaladnak a biometrikus ellenőrzőpontokon, QR-kódjukat egy QR-szkennerrel és kamerával felszerelt, erre a célra kialakított ellenőrzőegységnél mutatják fel. Az utas indexét az adatbázisba küldve lekérik a titkosított sablont, amelyet letöltve lokálisan ellenőriznek az ellenőrző egységen (pod) és/vagy a felhasználó eszközén. Az ellenőrzőpont adatkezelője csak a megfeleltetés eredményét ismeri meg és használja fel[87].

52. Ennél a forgatókönyvnél az azonosító és biometrikus adatok nem áramlanak a repülőterek között, és a központi adatbázisok között sem összeköttetés, sem interoperabilitás nem valósul meg.

Az Európai Adatvédelmi Testület értékelése

53. A 2. forgatókönyvnél az utasok regisztrált biometrikus sablonjait központosítottan, de titkosított formában tárolják, és azokhoz kizárólag az utasnál lévő kulcsot vagy titkos adatot társítanak. A 2. forgatókönyvnél az utasokat hitelesítik (1:1 összehasonlítással).

54. E forgatókönyv szerint az utasforgalom egyszerűsítésének célja (az ellenőrzések sebességének növelésével) egy központosított rendszer alkalmazásával lenne elérhető. A Testület korábban már megjegyezte, hogy ez a megoldás a regisztrált biometrikus sablonok decentralizált (az 1. forgatókönyv szerinti) tárolásával szemben megvalósítható alternatívának tekinthető[88], amennyiben erre objektív igény mutatkozik, és megfelelő biztosítékok állnak rendelkezésre (ezek ismertetését lásd az alábbi 60. bekezdéstől).

55. Ami a biztonsági szempontokat illeti, minden egyén adatait titkosítják a kizárólag az adott egyénnél tárolt és kizárólagos ellenőrzése alatt tartott egyedi kulccsal. Emellett az, hogy a megfeleltetéshez szükséges információkat (a titkos adatot vagy kulcsot) az egyénnek kell megadnia, második faktorként szolgál[89], és ezáltal erősíti a hitelesítés biztonságát. Emellett a titkosítás második rétegéről a repülőtér-üzembentartó gondoskodik az általa ellenőrzött kulcsokkal. A 2. forgatókönyvnél az egyén indexét a központi adatbázisba küldve kérik le az egyénhez társított biometrikus adatokat. Ezt követően ezeket az adatokat – titkosítva – az ellenőrzőponton található számítógépre küldik, ahol megfeleltetés céljából dekódolják azokat, az ellenőrzőpont adatkezelője viszont csak a megfeleltetés eredményét ismeri meg és használja fel. Feltéve, hogy az adott egyén kulcsát, illetve titkos adatát az ellenőrzőponti

[85] A francia felügyeleti hatóság pontosította, hogy a szükséges információk más technikai megoldással, például rövid hatótávolságú kommunikációs protokoll használatával is elküldhetők.
[86] Magát az egyénnél tárolt kulcsot vagy titkos adatot egy másik, a repülőtér-üzembentartó birtokában lévő kulccsal titkosítják.
[87] A francia felügyeleti hatóság tisztázta, hogy a szemléltető jelleggel közölt adattárolási időtartam elfogadhatónak tekinthető, mivel a kulcs az egyénnél van, és akár a regisztráció szakaszában is megválasztható. Meg kell azonban jegyezni, hogy az adattárolás időtartama kiigazítható.
[88] Az Európai Adatvédelmi Testület videoeszközökről szóló 3/2019. sz. iránymutatása, 88. bekezdés.
[89] Ez például csökkenti a személyazonossággal való visszaélés kockázatát. Lásd még a C.1.2. biztosítékot.

számítógépen lokálisan tárolják, és a titkosított biometrikus sablon lekérése céljából csak az utas indexét küldik a központi adatbázisba, az ilyen biztonsági intézkedések összeegyeztethetőnek tekinthetők az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával és 32. cikkével.

56. Ami az általános adatvédelmi rendelet 25. cikkével való összeegyeztethetőséget illeti, és különösen az adattakarékosság követelményének való megfelelés érdekében biztosítani kell, hogy az adatkezelés megfeleljen a szükségesség elvének. A 2. forgatókönyv esetében a választott intézkedések a kitűzött céllal (a repülőtéri utasforgalom egyszerűsítésével) összefüggésben akkor tekinthetők a szükségesség elvének megfelelőnek, ha az adatkezelés körülményeitől függően az adatkezelő bizonyítani tudja, hogy nincsenek olyan kevésbé intruzív alternatív megoldások, amelyekkel ugyanaz a cél hatékonyan elérhető. Az utasoknak a 2. forgatókönyv szerint is be kell mutatniuk az eszközüket[90]. Ennek ellenére az adatkezelő bizonyíthatja, hogy a 2. forgatókönyv felgyorsítja az ellenőrzési folyamatot mind az 1. forgatókönyvhöz, mind pedig a jelenlegi helyzethez képest, ahol emberi ellenőrzés keretében vizsgálják, hogy a beszállókártyán szereplő név egyezik-e az utas személyazonosító okmányával[91]. Ez ugyanis nem állapítható meg akkor, ha jelenleg nem végeznek ellenőrzéseket az utasok személyazonosságának a hivatalos személyazonosító okmányuk alapján történő igazolására (lásd e tekintetben a fenti 18. pontot).

57. Az arányosság elvét illetően az adatkezelés intruzív jellegét ellensúlyozhatja az utasok aktív részvétele, akik kizárólagos ellenőrzésük alatt tartják a titkosított adataikhoz tartozó kulcsot. Úgy tűnik továbbá, hogy az utasok biometrikus adatainak központosított adatbázisban, kizárólag az utasoknál lévő kulcsokkal társítva történő tárolásával járó biztonsági kockázatok csökkenthetők megfelelő biztosítékok alkalmazásával (ezek tárgyalását lásd az alábbi 60. bekezdéstől). Feltételezve tehát, hogy az adatkezelő megfelelő, a szóban forgó konkrét adatkezelés által megkövetelt biztosítékokat érvényesít, az egyéneket fenyegető kockázatok csökkenthetők, és az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás arányosnak tekinthető a várt haszonnal. Természetesen minden esetben biztosítani kell, hogy csak a célhoz szükséges adatok kezelésére kerüljön sor, és csak a hozzájárulásukat adó utasokat ellenőrizzék, ezáltal elkerülhető legyen annak a kockázata, hogy más utasok biometrikus adatait is gyűjtik, akik ehhez nem járultak hozzá.

58. A kérelemben példaként szerepel, hogy a 2. forgatókönyv szerint a titkosított adatok adatbázisban való tárolásának időtartama jellemzően az egyén utolsó útjától számított egy évig, legfeljebb az útlevél érvényességének lejártáig terjedhet. A kérelemben nem szerepel olyan információ, amely objektív okokkal alátámasztaná ezt a hosszú időtartamot, bár feltételezhető, hogy az adattárolás időtartamát kényelmi szempontból, a jövőbeli utakra tekintettel irányozzák elő. Az adattárolás időtartamát illetően az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontjával való összeegyeztethetőség elérése érdekében az adatkezelőknek meg kell tudniuk indokolni, hogy a konkrét esetekben miért van szükség az előirányzott adatmegőrzési időre. A Testület azt ajánlja az adatkezelőknek, hogy a lehető legrövidebb adattárolási időtartamot irányozzák elő, figyelembe véve azokat az utasokat is, akik csak

[90] A francia felügyeleti hatóság pontosította, hogy a sablon más módon, például papírra nyomtatva is bemutatható. Emellett a Testület elismeri, hogy a jövőben alternatív technológia alkalmazását lehetne előirányozni, például kis hatótávolságú kommunikációs rendszer alapján.

[91] Elmondható továbbá, hogy a biometrikus ellenőrzésnél kisebb valószínűséggel fordulnak elő hibák az emberi ellenőrzéshez képest.

nagyon ritkán repülnek, és kínálják fel az érintettek számára azt a lehetőséget, hogy meghatározzák az általuk preferált adattárolási időtartamot.

59. E szempontokra fényében a 2.1.1. kérdésre válaszolva a Testület arra a következtetésre jut, hogy az adatkezelés – **megfelelő biztosítékok mellett – elvben összeegyeztethetőnek tekinthető az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével**.

Megfelelő biztosítékok

60. Ilyen típusú forgatókönyv esetén a 2.1.2. kérdésre válaszolva a Testület **az 1. forgatókönyvnél felsoroltak mellett** legalább az alábbi biztosítékok érvényesítését tartja szükségesnek. *A jelen véleményben leírtaktól eltérő biztosítékok alkalmasak lehetnek ugyanazon biztonsági és adatvédelmi célok elérésére, emellett jogszerűek is lehetnek, amennyiben biztosítják az alkalmazandó jogi kereteknek való megfelelést.*

61. Megjegyzés: *az alábbiakban általános, nem teljes körű áttekintés található olyan megfelelő biztosítékokról, amelyeket az adatkezelőnek a 2. forgatókönyvhöz hasonló megoldás esetén érvényesíthet. Az általános adatvédelmi rendelet 25. és 32. cikke szerinti megfelelőségük esettől függően állapítható meg. Valamennyi adatkezelőnek gondoskodnia kell saját adatvédelmi hatásvizsgálat elvégzéséről, és konkrét megoldásaik további, ebben a véleményben nem szereplő intézkedéseket tehetnek szükségessé.*

D. Általános szempontok

D.1. Az érintettek jogai és az adatkezelők által érvényesíthető biztosítékok

D.1.1. Biztosítani kell, hogy az utas valamennyi adata tekintetében rendelkezzen az adattárolási időtartamról. Az adattárolási időtartamokat az adott cél eléréséhez szükséges mértékre kell korlátozni. Maximális időtartamot kell meghatározni olyan tényezők alapos elemzésének eredményeként, mint a személyazonosító okmány érvényessége. Az érintettek számára fel kell ajánlani az általuk preferált adattárolási időtartam meghatározását, amely rövidebb lehet az alapértelmezett időtartamnál.

D.1.2. Az érintett számára lehetővé kell tenni, hogy bármikor kérje a kizárólag nála, mobilalkalmazásban vagy digitálisadat-tárcában tárolt adatok (kulcs, titkos adat) törlését[92].

D.1.3. Biztosítani kell, hogy a központi adatbázis elhelyezése tegye lehetővé az illetékes felügyeleti hatóság általi hatékony felügyeletet.

[92] Ez a biztosíték csak a 2. forgatókönyvre vonatkozik.

E. Szervezeti szempontok:

E.1. Szabályozás és megfelelés

E.1.1. A központi szerver csak korlátozottan tekinthető megbízhatónak. Annak biztosítása, hogy a központi szerver irányítása világosan meghatározott irányítási szabályokat követ, és magában foglalja a szerver biztonságának garantálásához szükséges valamennyi intézkedést[93].

F. Műszaki szempontok:

F.1. Hozzáférés

F.1.1. Nyilvántartást kell vezetni arról, hogy ki fér hozzá személyes adatokhoz, különösen az azonosító és biometrikus adatokhoz, valamint a hozzáférés időpontjáról.

F.2. Infrastruktúra és hálózat

F.2.1. Garantálni kell a központi adatbázis megfelelő biztonságát, többek között a rendelkezésre állási támadásokkal szemben is.

F.2.2. Biztosítani kell, hogy ne legyen internetkapcsolat a központi adatbázissal, a regisztrációs egységekkel és a megfeleltetési egységekkel. A rendszer üzemeltetését és karbantartását (pl. biztonsági mentés, javítás, monitorozás stb.) helyi szinten, a repülőtér területén kell elvégezni.

F.3. Adatbiztonság és -kezelés

F.3.1. A legkorszerűbb kriptográfiai technikák bevezetése az alkalmazás és a központi szerver közötti információcsere biztonsága érdekében[94].

F.3.2. Az egyedi kulcsot vagy titkos adatot azon a szinten kell tartani, ahol azt dekódolásra használják (az ellenőrző egység szintjén), a központi adatbázisban tárolt, regisztrált biometrikus sablon lekérése csak az index segítségével történhet.

F.3.3. A kulcs, illetve titkos adat felhasználói eszköz és ellenőrző egység közötti adatcsere során biztosítani kell az esetleges lehallgatással vagy harmadik félnek történő továbbítással szemben védett kommunikációt.

[93] Az Európai Adatvédelmi Testület 4/2020 sz. iránymutatása a helymeghatározó adatokról és a kontaktkövető eszközökről, PRIV-5, 17. o.

[94] Az Európai Adatvédelmi Testület 4/2020 sz. iránymutatása a helymeghatározó adatokról és a kontaktkövető eszközökről, SEC-4, 16. o.: „Az alkalmazható technikák közé tartoznak például a következők: szimmetrikus és aszimmetrikus titkosítás, hash-funkciók, bizalmas tagsági teszt (PMT), bizalmas metszetképzés, Bloom-szűrők, bizalmas információk visszakeresése, homomorfikus titkosítás”.

F.3.4. A központi adatbázisban tárolt biometrikus sablont indexálni kell az 1:1 hitelesítés lehetővé tétele, valamint a sablon egyedisége és egyénhez társítása érdekében. Biztosítani kell, hogy az index ne fedje fel az utas azonosító adatait, és ne korreláljon a titkosítási kulccsal.

F.3.5. A központi adatbázis és az ellenőrzőpontok közötti adattovábbítást megfelelő hitelesítés és titkosítás mellett, izolált hálózatokban kell végezni.

F.3.6. Az adatkészletek (az azonosító és biometrikus adatok, valamint a járatadatok) közötti kétirányú kapcsolatokat kerülni kell, az adatbázisban csak a releváns egyirányú kapcsolatok tárolhatók. Például csak az indexről az azonosítóra, az indexről a titkosított biometrikus adatokra, valamint az indexről a járatadatokra mutató kapcsolatok tárolása megengedett.

F.3.7. Gondoskodni kell az üzletmenet-folytonosságról, például megfelelő tartalék tárolórendszerek révén.

F.3.8. Biztosítani kell, hogy az ellenőrző egység ne naplózza a titkosított vagy titkosítatlan sablonokat.

3.2.3 A regisztrált biometrikus sablonok központosított tárolása azonosítás céljából

62. Ez a szakasz azt vizsgálja, hogy az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjával, valamint 25. és 32. cikkével összeegyeztethető-e az utasok regisztrált biometrikus sablonjának központosított, titkosított formában történő tárolása azonosítás céljából, a kizárólag az utasnál lévő kulccsal vagy titkos adattal történő titkosítás nélkül, az alábbi két gyakorlati példán keresztül: 1. a sablonokat a repülőtér-üzemeltető ellenőrzése alatt a repülőtéren található adatbázisban tárolják[95] (a továbbiakban: **3.1. forgatókönyv**), valamint 2. a sablonokat a légitársaság ellenőrzése alatt, felhőben tárolják[96] (a továbbiakban: **3.2. forgatókönyv**).

63. A Testület úgy véli, hogy a biometrikus adatoknak a nagy központi adatbázisokban **azonosítási** célokra történő felhasználása sérti az érintettek alapvető jogait, és súlyos következményekkel járhat az érintettek számára[97]. Ezenkívül a biometrikus adatok felhasználását az adatkezelés céljával összefüggésben, a szükségesség és az arányosság elvének fényében is vizsgálni kell[98].

[95] A kérelem I. mellékletében szereplő 3A. használati eset példáján keresztül.
[96] A kérelem I. mellékletében szereplő 3B. használati eset példáján keresztül.
[97] Lásd például a 29. cikk szerinti munkacsoport biometrikus technológiákról szóló 3/2012. sz. véleményét, 8. o. Lásd még a fenti 26. bekezdést.
[98] Az általános adatvédelmi rendelet (4) preambulumbekezdése. Lásd még a 29. cikk szerinti munkacsoport biometrikus technológiákról szóló 3/2012. sz. véleményét, 8. o.

3.2.3.1 3.1. forgatókönyv: Központosított tárolás a repülőtéren belüli adatbázisban, a repülőtér-üzembentartó ellenőrzése alatt

A forgatókönyv ismertetése

64. A 3.1. forgatókönyv szerint az utasok regisztrált biometrikus sablonját a repülőtér területén található központi adatbázisban, a repülőtér-üzembentartó ellenőrzése alatt, titkosított formában tárolják. Az utasok adatait csoportokba sorolják , ami azt jelenti, hogy azonosító adataikat, regisztrált biometrikus sablonjukat és járatadataikat három különböző adatbázisban tárolják. Ezeket az adatokat különböző kulcsokkal titkosítják, mind a tárolás során, mind pedig a megfeleltetést végző szerverekhez történő továbbításuk során, ahol a repülőtér üzemeltetője dekódolja azokat.

65. Az utasoknak az indulás előtt rövid időn belül (pl. 48 órával) minden járatra regisztrálniuk kell. A regisztráció történhet távolról vagy olyan repülőtéri terminálokon keresztül, amelyek a személyazonosság tekintetében megfelelő szintű bizonyosságot nyújtanak (pl. az eIDAS szerint). Alternatív megoldásként a regisztráció az 1. forgatókönyvnél leírt formát öltheti, amely esetben az utasoknak az indulásuk előtt 48 órán belül el kell juttatniuk adataikat a digitálisadat-tárcájukból a repülőtéri rendszerbe.

66. Az utasok ennél a forgatókönyvnél is egy erre a célra kialakított, kamerával felszerelt ellenőrzőegység előtt haladnak el. Biometrikus mintájukat ezután egy központi repülőtéri szerverre küldik, amely megpróbálja megfeleltetni az adatokat a központi biometrikus adatbázis adatainak. Az utas így azonosítható és ellenőrizhető, hogy valóban regisztrálták-e egy induló járatra (vagy a beszálláskor történő ellenőrzés esetén a beszállítást végző járatra). Az ellenőrzőponttól függően a lekérdező ellenőrzőponti adatkezelőnek visszaküldött adatok minimalizálhatók, például „igen/nem” válasz formájában, szükség esetén pedig a megfeleltetés eredményeként. Ebben az esetben az ellenőrzőpont adatkezelője csak a kérés eredményét kapja meg és használja fel.

67. Ennél a forgatókönyvnél az utasokat azonosítják (1:N összehasonlítással), ahol N a repülőtéren több napon belül várható utasok száma. A biometrikus megfeleltetésre továbbá csak akkor kerül sor, ha az adott utas megjelenik az indulási repülőtér előre meghatározott ellenőrzőpontjain, maga az adatkezelés pedig a központi adatbázishoz kapcsolódó központi szerveren történik. Ebben a forgatókönyvben az adattárolási időtartam jellemzően 48 óra, és az adatokat a repülőgép felszállását követően törlik.

Az Európai Adatvédelmi Testület értékelése

68. Amint arra fentebb emlékeztettünk, a biometrikus adatok kezelése fokozott kockázatokkal jár az érintettek jogaira és szabadságaira nézve[99]. Így az adatbiztonság bármely hiányossága különösen súlyos következményekkel járhat az érintettekre nézve[100]. Az adatkezelők kötelesek hatékonyan csökkenteni ezeket a kockázatokat. Mivel ennél a forgatókönyvnél az architektúra egésze teljesen központosított, az utasok nagyobb mértékben veszítik el adataik feletti rendelkezést. Ezenkívül

[99] Lásd a fenti 26. bekezdést.

[100] Az Európa Tanács a személyes adatok kezelése vonatkozásában a természetes személyek védelmére vonatkozó egyezménnyel foglalkozó konzultatív bizottságának iránymutatásai, 2021. június, 22. o.

nagyobb lehet annak a kockázata is, hogy az adatokat az utasforgalom irányításától eltérő egyéb célból kezelik.

69. A biztonságra vonatkozó elv és követelmények (az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontja és 32. cikke) fényében figyelembe kell venni, hogy az azonosító és biometrikus adatok központi – bár különálló – adatbázisokban való tárolása jelentős támadási felületet nyithat, és az ilyen adatbázisok bizalmas jellegének megsértése pedig a későbbiekben a teljes adatkészlethez való hozzáférést vonhatja maga után. Következésképpen az arcfelismerő sablonok és a kapcsolódó azonosító adatok esetleges megsértése lehetővé teheti az érintettek illetéktelen vagy jogellenes azonosítását más környezetben. A biometrikus azonosításhoz használt módszerektől függően az arcfelismerő sablonok azonosítóként való további biztonságos használatát is veszélyeztetheti. Ebben az esetben az adatvédelmi incidens hatásai nem enyhíthetők, ellentétben más típusú hitelesítő adatokkal (pl. felhasználó azonosítóval, jelszóval), amelyek módosíthatók[101].

70. Emellett az adatkezelő birtokában lévő azonosító és biometrikus adatok nagy mennyisége és jó minősége az adatkészletet igen értékes célponttá teszi a támadók számára, ami a biztonsági kockázat szempontjából fokozott valószínűséget jelent. Ezen túlmenően az adatvédelmi incidenseknek súlyosabb kihatásai lehetnek, mivel az adatok központosított helyen való tárolása miatt a támadók könnyebben férhetnek hozzá több utasra vonatkozó személyes adatokhoz. Ezért egy esetleges adatvédelmi incidens potenciálisan nagy számú érintettet tehetne ki olyan, a súlyosság tekintetében magas kockázatoknak, mint például a tömeges személyazonosság-lopás, amelyeket rendkívül nehéz mérsékelni.

71. Ezért az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával és 32. cikkével való összeegyeztethetőség tekintetében a 3.1. forgatókönyvben előirányzott intézkedések[102] – figyelembe véve a technika állását – nem elegendőek a kockázatnak megfelelő biztonsági szint biztosításához. Ennek alapján a 3.1. forgatókönyv szerinti adatkezelés nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának és 32. cikkének, ha az adatkezelő a forgatókönyv szerinti intézkedésekre szorítkozna.

72. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontjában foglalt elv fényében ebben a forgatókönyvben a biometrikus adatok központi adatbázisban való tárolásának időtartama jellemzően 48 óra. Ez a korlátozott tárolhatóság jelentősen csökkenti a személyes adatok megsértésével kapcsolatos kockázatokat. Mindazonáltal az adattárolási időtartam önmagában nem döntő tényező az említett architektúra általános összeegyeztethetősége szempontjából, mivel az adatmegőrzési időket az adatkezelők módosíthatják. A javasolt intézkedéseknek minden esetben meg kell felelniük az általános adatvédelmi rendelet 25. cikke szerinti beépített és alapértelmezett adatvédelem követelményeinek.

73. Az 1. és 2. forgatókönyvvel ellentétben, ahol az utasokat hitelesítik, a 3.1. forgatókönyv esetében az utasokat azonosítják (1:N összehasonlítással), itt N a repülőtéren egy többnapos időkereten belül várható utasok száma, akik hozzájárultak a meghatározott repülőtéri ellenőrzőpontokon való áthaladáskor végzett adatkezeléshez. Ez azt jelenti, hogy az utasokat egy központi adatbázisban kell

[101] Ennek kapcsán lásd a 29. cikk szerinti munkacsoport biometrikus technológiákról szóló 3/2012. sz. véleményét, 34. o.
[102] A fenti 64–67. bekezdésben leírtak szerint.

lekérdezni oly módon, hogy minden egyes rögzített biometrikus mintát feldolgoznak annak ellenőrzése érdekében, hogy egyeznek-e a rendszerben ismert személlyel. A 2. forgatókönyvvel szemben a 3.1. forgatókönyv esetében a kulcsok nem kizárólag az utasoknál vannak. Következésképpen ennél a forgatókönyvnél az utasok lényegesen kevesebb ellenőrzéssel bírnak biometrikus adataik felett. Ezért a 3.1. forgatókönyv esetében a tervezett adatkezelés nem egyeztethető össze az általános adatvédelmi rendelet 25. cikke szerinti, a beépített adatvédelemre vonatkozó és kialakítási követelményekkel.

74. Az általános adatvédelmi rendelet 25. cikkének fényében az adatkezelőknek figyelembe kell venniük az adatkezeléshez szükséges személyes adatok típusait, kategóriáit és részletességét[103]. Az adatkezelőknek a kialakítással kapcsolatos döntéseik során figyelembe kell venniük az adattakarékosság, az integritás és a bizalmas jelleg, valamint a korlátozott tárolhatóság elvére jelentett fokozott kockázatot a nagy mennyiségű, részletes személyes adatok gyűjtése során, és ezt a kockázatot össze kell vetniük az érintettekkel kapcsolatos kevesebb és/vagy kevésbé részletes információk gyűjtése által jelentett kisebb kockázattal. Az alapértelmezett beállítás semmiképpen nem foglalhatja magában olyan személyes adatok gyűjtését, amelyek nem szükségesek a konkrét adatkezelési cél eléréséhez. Más szóval, ha a személyes adatok bizonyos kategóriái szükségtelenek, vagy ha részletes adatokra azért nincs szükség, mert kevésbé részletes adatok is elegendőek, a felesleges személyes adatok nem gyűjthetők. Ebben az esetben nem szükséges arcfelismerő technológiát alkalmazni, ha más adatkezelési megoldással ugyanaz a cél elérhető, és az a 3.1. forgatókönyvben leírt feltételek szerint rendelkezésre áll.

75. Az általános adatvédelmi rendelet 25. cikkét illetően a beépített és alapértelmezett adatvédelem egyik fő eleme az érintett autonómiája. Ebben a tekintetben, az érintett számára a lehető legnagyobb mértékű autonómiát kell biztosítani a személyes adataik felhasználása, továbbá a felhasználás és az adatkezelés körének és feltételeinek tekintetében[104]. Az 1. forgatókönyvnél az érintett autonómiával és ellenőrzéssel rendelkezne biometrikus sablonja használata, átadása és törlése tekintetében, a 2. forgatókönyv esetében pedig az érintett bizonyos fokú ellenőrzést tartana fenn saját biometrikus sablonjának átadása tekintetében, mivel a titkosítási kulcs, illetve titkos adat tárolása nála történik. A 3.1. forgatókönyv szerint azonban az érintett teljes mértékben függ a biometrikus adatainak kezelésével kapcsolatos adatkezelői döntésektől, és ezért nincs közvetlen ellenőrzése a biometrikus sablon használata felett.

76. Az általános adatvédelmi rendelet 25. cikkével való összeegyeztethetőség, és különösen az adattakarékosság követelményének való megfelelés szempontjából a 3.1. forgatókönyv szerint tervezett adatkezelés nem tud megfelelni a szükségesség elvének. A Testület úgy véli, hogy a repülőterek utasforgalmának egyszerűsítése tekintetében hasonló eredmény kevésbé intruzív módon is elérhető. Elérhető például biometrikus adatok használata nélkül is (bár ekkor a felhasználói élmény eltérő lenne, mivel hosszabb időt vehet igénybe a beszállókártya és szükség esetén a hivatalos személyazonosító okmányok bemutatása). Továbbá más megoldások, nevezetesen a biometrikus adatoknak az egyén eszközén található helyi adattárcában történő tárolására támaszkodó

[103] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a beépített és alapértelmezett adatvédelemről, 49. bekezdés.

[104] Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a beépített és alapértelmezett adatvédelemről, 70. bekezdés. Az általános adatvédelmi rendelet (7) preambulumbekezdése továbbá egyértelművé teszi, hogy „[a] természetes személyek számára biztosítani kell, hogy saját személyes adataik felett maguk rendelkezzenek”.

megoldások, vagy az adatoknak az egyén eszközén tárolt konkrét kulcs segítségével történő titkosítását igénylő megoldások lehetővé teszik a célok kevésbé intruzív módon történő elérését.

77. Ami az arányosság elvét illeti, a 3.1. forgatókönyvben előirányzott adatkezelés olyan kockázatokat jelentene az érintettek jogaira nézve, amelyeket a technika jelenlegi állása miatt a tervezett intézkedések nem mérsékelnének. Az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás, amelyet a nagyszámú egyén biometrikus adatait tartalmazó központi adatbázisban előforduló adatvédelmi incidens okozhat, feltehetően meghaladja az adatkezelésből származó várható hasznot, mivel ez az előny viszonylag csekély: az ellenőrzések kényelme és gyorsasága nő kismértékben. Ennélfogva nem igazolhatja az ezen intézkedések által az egyének alapvető jogaiban és szabadságaiban okozott jelentős sérelmet, és a 3.1. forgatókönyvben előirányzott adatkezelés nem felel meg az arányosság elvének.

78. E megfontolások fényében a 2.2.1. kérdésre válaszolva a Testület arra a következtetésre jut, hogy amennyiben az adatkezelés kifejezetten a repülőterek utasforgalmának egyszerűsítése céljából történik, a 3.1. forgatókönyvben előirányzott adatkezelés:

- **nem összeegyeztethető az általános adatvédelmi rendelet 25. cikkével**,
- **nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának és 32. cikkének**, ha az adatkezelő a 3.1. forgatókönyvben leírt intézkedésekre szorítkozna.

3.2.3.2 3.2. forgatókönyv: központosított tárolás felhőben, a légitársaság ellenőrzése alatt

A forgatókönyv ismertetése

79. A 3.2. forgatókönyv szerint az utasok regisztrált biometrikus sablonját a felhőben tárolják a légitársaság vagy felhőszolgáltatója (adatfeldolgozó) ellenőrzése alatt. A kérelemben leírtak szerint a felhőszolgáltató székhelye az EGT területén lenne[105]. Ebben az esetben az utasok adatait titkosítják, de használat közben (például a megfeleltetési művelet végrehajtásakor) dekódolják, és a kulcsokat a légitársaság vagy adatfeldolgozóként annak felhőszolgáltatója ellenőrzi. Az utasok biometrikus adatait az utasok azonosítására használják (1:N összehasonlítással), ahol N a légitársaság összes ügyfelének számáig terjedhet[106].

80. Az 1., 2. és 3.1. forgatókönyvhöz hasonlóan az utasoknak először itt is regisztrálniuk kell. A 3.2. forgatókönyv szerint azonban az utasok regisztrációjára egyszer kerül sor, és az mindaddig érvényes, amíg az ügyfél fiókkal rendelkezik a légitársaságnál. A regisztráció távolról, a személyazonosság tekintetében megfelelő szintű bizonyosság mellett (pl. az eIDAS szerint) vagy a repülőtéri terminálokon történik. A biometrikus megfeleltetésre csak akkor kerül sor, ha az utas megjelenik a repülőtér előre meghatározott ellenőrzőpontjain, maga az adatkezelés pedig a felhőben történik.

81. A repülőtéren az utasok erre a célra kialakított, kamerával felszerelt ellenőrzőegység előtt haladnak el. Az utasok biometrikus adatait kérés útján továbbítják a légitársaság felhőszerveréhez, ahol ezeket az adatokat összevetik a központi adatbázissal. Az utas így azonosítható és ellenőrizhető, hogy valóban regisztrálták-e egy induló járatra (vagy beszállási járatra beszálláskor történő ellenőrzés esetén).

82. Az egyező eredmények potenciálisan több repülőtér-üzemeltető számára is hozzáférhetővé tehetők, ha a légitársaság külön terminállal vagy hozzáféréssel rendelkezik egy repülőtér közös információs infrastruktúrájához. Az ellenőrzőponttól függően a lekérdező ellenőrzőponti adatkezelőnek visszaküldött adatok minimalizálhatók, például „igen/nem” válasz formájában, szükség esetén pedig a megfeleltetés eredményeként. Ebben az esetben az ellenőrzőpont adatkezelője csak a kérés eredményét ismeri meg és használja fel.

83. A sablon adattárolási időtartamát a légitársaság határozza meg, és az potenciálisan addig tarthat, amíg az ügyfél fiókkal rendelkezik a légitársaságnál.

Az Európai Adatvédelmi Testület értékelése

84. A Testület által a 3.1. forgatókönyvvel kapcsolatban már kifejtett megfontolások[107] erre a forgatókönyvre is érvényesek.

---

[105] A francia felügyeleti hatóság tisztázta, hogy a szemléltető jelleggel leírt eset mellett elképzelhetők olyan felhőszolgáltatók is, amelyek nem az EGT területén találhatók. Emellett más tárolási megoldások is elképzelhetők (pl. felhő használata nélkül).

[106] A francia felügyeleti hatóság tisztázta, hogy a szemléltető jelleggel leírt eset mellett olyan megoldás is létezik, ahol a biometrikus adatokkal a járat indulása előtt minden alkalommal *push* műveletet végeznek.

[107] Lásd a fenti 68–77. pontot.

85. Ami a biztonságra vonatkozó elvet és követelményeket (az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontja és 32. cikke) illeti, a 3.2. forgatókönyv szerinti adatkezelés a felhőben történik, és több szervezet is hozzáférhet ezekhez az adatokhoz, beleértve esetleg az EGT-n kívüli szolgáltatókat, még akkor is, ha az adatokat az EGT területén tárolják[108]. Ez az architektúra a személyes adatok harmadik országokba történő továbbításának lehetséges kockázatát rejti magában. Ezen túlmenően, bár az utasok adatait titkosítják, a felhasználás során (a megfeleltetési művelet végrehajtásakor) dekódolják, a kulcsokat pedig a légitársaság vagy adatfeldolgozóként annak felhőszolgáltatója ellenőrzi. Ez a tárolási mód tovább növeli a lehetséges biztonsági sérülés felületét.

86. Ezért az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával és 32. cikkével való összeegyeztethetőség tekintetében a 3.2. forgatókönyvben előirányzott intézkedések[109] – figyelembe véve a technika állását – nem elegendőek a kockázatnak megfelelő biztonsági szint biztosításához. Ennek alapján a 3.2. forgatókönyv szerinti adatkezelés nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának és 32. cikkének, ha az adatkezelő a forgatókönyv szerinti intézkedésekre szorítkozna.

87. Ezenkívül a 3.2. forgatókönyv szerint[110] az adatok jelentős ideig tárolhatók (akár mindaddig, amíg az érintett fiókkal rendelkezik a légitársaságnál). A hosszabb tárolási időtartam az adatokat a bizalmasság és az integritás szempontjából az incidens nagyobb kockázatának teszi ki, és feltehetően meghaladja az adatkezelés céljához feltétlenül szükséges és arányos mértéket. A Testület megjegyzi, hogy az említett architektúra általános adatvédelmi rendelettel való általános összeegyeztethetősége szempontjából az adattárolási időtartam önmagában nem döntő tényező, mivel azt az adatkezelők módosíthatják. A Testület rendelkezésére álló és a 3.2. forgatókönyv leírásában szereplő információk alapján azonban ez a hosszú adattárolási időtartam nem indokolt, emellett nyilvánvaló intézkedések sincsenek az egyéneket érintő kockázatok csökkentésére. Ennek alapján az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontjában foglalt korlátozott tárolhatóság elve értelmében a tervezett adattárolási időtartam nem korlátozódna a szükséges mértékűre.

88. Mindenesetre a 3.2. forgatókönyv szerint javasolt intézkedésekkel nem teljesíthetők az általános adatvédelmi rendelet 25. cikkében foglalt beépített és alapértelmezett adatvédelmi követelmények. A 3.2. forgatókönyv szerint az utasok regisztrált biometrikus sablonjait a felhőben tárolják a légitársaság vagy felhőszolgáltatója (adatfeldolgozó) ellenőrzése alatt. A fentiek szerint több jogalany is hozzáférhet ezekhez az adatokhoz. Az utasok biometrikus adatait továbbá az utasok azonosítására használják (1:N

89. összehasonlítással), ahol N a légitársaság összes felhasználójának, illetve ügyfelének számáig terjedhet. A módszer szerint az egyén a központi adatbázisban rögzített csoporton belül úgy található meg, hogy minden egyes rögzített arcot feldolgozva ellenőrzik a rendszerben ismert személlyel való egyezést. A 3.1. forgatókönyvvel ellentétben a 3.2. forgatókönyv esetében az összehasonlítás sokkal nagyobb léptékben is végezhető, mivel itt a légitársaság összes ügyfelének száma a kritérium, míg a 3.1. forgatókönyv csak a többnapos időkereten belül várható utasok számát veszi alapul.

[108] Az Európai Adatvédelmi Testület 2022. évi online ellenőrzési akciója a felhőalapú szolgáltatások közszektorbeli használata terén, 2023. január 17., 19. o.
[109] Lásd a fenti 79–83. pontot.
[110] Lásd a fenti 83. pontot.

90. Ezenfelül ami az általános adatvédelmi rendelet 25. cikkével való összeegyeztethetőséget illeti, és különösen az adattakarékosság követelményének való megfelelés tekintetében a 3.2. forgatókönyv szerint tervezett adatkezelés nem felel meg a szükségesség elvének. A Testület úgy véli, hogy a repülőterek utasforgalmának egyszerűsítése tekintetében hasonló eredmény kevésbé intruzív módon is elérhető, akár biometrikus adatok használata nélkül is (bár ekkor a felhasználói élmény eltérő lenne, mivel hosszabb időt vehet igénybe a személyazonosító okmányok és a beszállókártya bemutatása). Továbbá más megoldások, nevezetesen a biometrikus adatoknak az egyén eszközén található helyi adattárcában történő tárolására támaszkodó megoldások, vagy az adatoknak az egyén eszközén tárolt konkrét kulcs segítségével történő titkosítását igénylő megoldások az adatkezelő számára lehetővé teszik a célok kevésbé intruzív módon történő elérését.

91. Ami az arányosság elvét illeti, a 3.2. forgatókönyvben előirányzott adatkezelés olyan kockázatokat jelentene az érintettek jogaira nézve, amelyeket az előirányzott biztosítékok nem mérsékelnének. Az érintettek alapvető jogaira és szabadságaira gyakorolt negatív hatás, amelyet a nagyszámú egyén felhőben tárolt biometrikus adatait tartalmazó központi adatbázisban előforduló adatvédelmi incidens okoz, feltehetően meghaladja az adatkezelésből származó várható hasznot, mivel ez az előny viszonylag csekély: az ellenőrzések kényelme és gyorsasága nő kismértékben. Ennélfogva nem igazolhatja az ezen intézkedések által az egyének alapvető jogaiban és szabadságaiban okozott jelentős sérelmet, és a 3.2. forgatókönyvben előirányzott adatkezelés nem tekinthető arányosnak.

92. E megfontolások fényében a 2.3.1. kérdésre válaszolva a Testület arra a következtetésre jut, hogy amennyiben az adatkezelés kifejezetten a repülőterek utasforgalmának egyszerűsítése céljából történik, a 3.2. forgatókönyvben előirányzott adatkezelés:

- **nem összeegyeztethető az általános adatvédelmi rendelet 25. cikkével**,
- **nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának és 32. cikkének**, ha az adatkezelő a 3.2. forgatókönyvben leírt intézkedésekre szorítkozna,
- **nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése e) pontjának**, mivel a Testület rendelkezésére álló információk alapján nem indokolt a 3.2. forgatókönyvben előirányzott megőrzési időszak. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontjában foglalt korlátozott tárolhatóság elvének való megfelelés érdekében az adatkezelőnek bizonyítania kell, hogy a személyes adatokat csak az adatkezelés céljaihoz szükséges ideig tárolják.

4 KÖVETKEZTETÉSEK

93. Az 1.1. kérdést illetően, a francia felügyeleti hatóság vélemény iránti kérelme nyomán, az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjában, 25. cikkében és 32. cikkében előírt követelményekkel kapcsolatban, a fenti elemzés alapján a Testület az alábbi következtetésre jut:

94. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének f) pontjával (az integritás és bizalmas jelleg elve), valamint 25. és 32. cikkével elvben összeegyeztethetőnek tekinthető az arcfelismerő technológia biometrikus alapú hitelesítésre, a repülőtéri utasforgalom egyszerűsítésének konkrét céljából (a biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor) történő alkalmazása olyan tárolási architektúra esetében, ahol az egyes utasok regisztrált biometrikus sablonját az adott egyénnél helyben, a kizárólagos ellenőrzése alatt lévő

személyes eszközön tárolják, a fenti 46. bekezdéstől leírtak szerinti megfelelő biztosítékok megléte esetén.

95. A 2.1.1. kérdést illetően, a francia felügyeleti hatóság vélemény iránti kérelme nyomán, az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjában, 25. cikkében és 32. cikkében előírt követelményekkel kapcsolatban, a fenti elemzés alapján a Testület az alábbi következtetésre jut:

96. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontjával (a korlátozott tárolhatóság elve), 5. cikke (1) bekezdésének f) pontjával (az integritás és bizalmas jelleg elve), valamint 25. és 32. cikkével elvben összeegyeztethetőnek tekinthető az arcfelismerő technológia biometrikus alapú hitelesítésre, a repülőtéri utasforgalom egyszerűsítésének konkrét céljából (a biztonsági ellenőrzőpontokon, a poggyászfelvételnél, beszálláskor, valamint a várókba történő belépéskor) történő alkalmazása olyan központosított tárolási architektúra esetében, ahol az egyes utasok regisztrált biometrikus sablonját a repülőtéren belül, a repülőtér-üzembentartó ellenőrzése alatt álló központi adatbázisban, titkosított formában, kizárólag az egyénnél tárolt kulccsal vagy titkos adattal hozzáférhetően tárolják, a fenti 60. bekezdéstől leírtak szerinti megfelelő biztosítékok megléte esetén.

97. A 2.2.1. kérdést illetően, a francia felügyeleti hatóság vélemény iránti kérelme nyomán, az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjában, 25. cikkében és 32. cikkében előírt követelményekkel kapcsolatban, a fenti elemzés alapján a Testület az alábbi következtetésre jut:

98. Nem összeegyeztethető az általános adatvédelmi rendelet 25. cikkével az arcfelismerő technológia biometrikus alapú azonosításra történő alkalmazása a repülőtéri utasforgalom egyszerűsítésének konkrét céljából (biztonsági ellenőrzőpontokon, poggyászfelvételnél, beszálláskor és a várókba történő belépéskor) központosított tárolási architektúra esetében, amennyiben az utasok regisztrált biometrikus sablonjait nem titkosítják kizárólag az egyes utasoknál lévő kulccsal vagy titkos adattal, amennyiben e sablonokat a repülőtéren található adatbázisban, a repülőtér-üzembentartó ellenőrzése alatt tárolják. Az adatkezelés emellett nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának (az integritás és bizalmas jelleg elve) és 32. cikkének, ha az adatkezelő a 3.1. forgatókönyvben leírt intézkedésekre szorítkozna.

99. A 2.3.1. kérdést illetően, a francia felügyeleti hatóság vélemény iránti kérelme nyomán, az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) és f) pontjában, 25. cikkében és 32. cikkében előírt követelményekkel kapcsolatban, a fenti elemzés alapján a Testület az alábbi következtetésre jut:

100. Nem összeegyeztethető az általános adatvédelmi rendelet 25. cikkével az arcfelismerő technológia biometrikus alapú azonosításra történő alkalmazása repülőtéri utasforgalom egyszerűsítésének konkrét céljából (biztonsági ellenőrzőpontokon, poggyászfelvételnél, beszálláskor és a várókba történő belépéskor) központosított tárolási architektúra esetében, amennyiben az utasok regisztrált biometrikus sablonjait nem titkosítják kizárólag az egyes utasoknál lévő kulccsal vagy titkos adattal, amennyiben e sablonokat felhőben, a légitársaság ellenőrzése alatt tárolják. Az adatkezelés emellett nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése f) pontjának (az integritás és bizalmas jelleg elve) és 32. cikkének, ha az adatkezelő a 3.2. forgatókönyvben leírt intézkedésekre szorítkozna. Végül a 3.2. forgatókönyv ismertetése, valamint a Testület rendelkezésére álló információk alapján az adatkezelés nem felelne meg az általános adatvédelmi rendelet 5. cikke (1) bekezdése e) pontjának (a korlátozott tárolhatóság elve).

Az Európai Adatvédelmi Testület részéről

az elnök

(Anu Talus)