Stanovisko č. 11/2024 k používání rozpoznávání obličeje pro zefektivnění toku cestujících na letištích (slučitelnost s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 obecného nařízení o ochraně osobních údajů)

Verze 1.1

Přijatá dne 23. května 2024

Přijato

Verze 1.1	28. května 2024	Gramatická oprava ve shrnutí (strany 3 a 4) a v odstavcích 77 a 90 stanoviska
Verze 1.0	23. května 2024	Přijetí stanoviska

Shrnutí

Francouzský dozorový úřad požádal Evropský sbor pro ochranu osobních údajů, aby vydal stanovisko k používání technologie rozpoznávání obličeje provozovateli letišť a leteckými společnostmi pro biometrické ověřování nebo identifikaci cestujících, jenž mají za cíl zefektivnit tok cestujících na letištích.

Na úvod sbor připomíná, že používání biometrických údajů, a zejména technologie rozpoznávání obličeje, s sebou nese zvýšená rizika pro práva a svobody subjektů údajů. Týká se zpracování biometrických údajů, kterým je podle článku 9 GDPR poskytována zvláštní ochrana. Před použitím těchto technologií, i kdyby byly považovány za zvláště účinné, by správci měli posoudit dopad na základní práva a svobody subjektů údajů a zvážit, zda lze legitimního účelu zpracování dosáhnout méně rušivými prostředky.

Rozsah tohoto stanoviska je na základě žádosti omezen na slučitelnost zpracování s **čl. 5 odst. 1 písm. e) a f) a s články 25 a 32 GPDR** za **konkrétním účelem zefektivnění toku cestujících na letištích** na čtyřech konkrétních kontrolních stanovištích, a to na stanovištích bezpečnostní kontroly, při odbavení zavazadel, při nástupu do letadla a při vstupu do haly pro cestující. Toto stanovisko neobsahuje úplnou a kompletní analýzu dodržování GDPR ze strany příslušných správců a případně i jejich zpracovatelů. Tímto stanoviskem proto není dotčena individuální právní a technická analýza, která je založena na konkrétním plánovaném zpracování ze strany správce a okolnostech zpracování tímto správcem. Do rozsahu otázek předložených sboru v žádosti navíc nespadá analýza použitelného právního základu, a proto se platnost souhlasu s takovým zpracováním v souladu s články 6, 7 a 9 GDPR v tomto stanovisku nezkoumá. Tímto stanoviskem navíc nejsou dotčena omezení používání biometrických údajů, která jsou stanovena v právních předpisech členských států.

V tomto stanovisku sbor posuzuje soulad zpracování s výše uvedenými ustanoveními GDPR v kontextu **čtyř konkrétních scénářů**.

První scénář zahrnuje uložení zaregistrované biometrické šablony v rukou fyzické osoby, například na jejím individuálním zařízení, které má pod svou výhradní kontrolou, aby bylo možné ověřit (porovnáním 1:1) cestujícího při průchodu výše uvedenými letištními kontrolními stanovišti.

Sbor dospěl k závěru, že zvolená opatření lze považovat za splňující zásadu nezbytnosti, pokud správce může prokázat, že neexistují alternativní řešení, která mají méně narušující povahu a která by mohla dosáhnout totožného cíle stejně účinně. Kromě toho může být narušující povaha zpracování vyvážena aktivním zapojením cestujících, protože jejich biometrická šablona je uložena pouze v jejich rukou, například na jejich individuálním zařízení, pod jejich výhradní kontrolou a jejich údaje jsou vymazány krátce po dokončení porovnávání. S ohledem na tyto skutečnosti dospěl sbor k závěru, že zpracování předpokládané v prvním scénáři **lze v zásadě považovat za slučitelné s čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR**, pokud budou zavedeny vhodné záruky.

Sbor určil záruky, které by měly být v minimálním rozsahu zavedeny v případě řešení, které se podobá prvnímu scénáři.

Druhý scénář zahrnuje centralizované uložení zaregistrované biometrické šablony v zašifrované podobě s klíčem / tajným heslem, které má v rukou výhradně cestující, v rámci letiště. To umožňuje ověřování cestujících (porovnáním 1:1) při průchodu výše uvedenými letištními kontrolními stanovišti.

Registrace je platná po určitou dobu, která může být dlouhá například až jeden rok od posledního letu do data vypršení doby platnosti pasu.

Sbor dospěl k závěru, že zpracování lze považovat za splňující zásadu nezbytnosti, pokud správce může prokázat, že neexistují alternativní řešení, která mají méně narušující povahu a která by mohla dosáhnout totožného cíle stejně účinně. Kromě toho může být narušující povaha zpracování vyvážena aktivním zapojením cestujícího, který má pod svou výhradní kontrolou klíč / tajné heslo ke svým zašifrovaným biometrickým údajům. Zavedením vhodných záruk ze strany správce lze bezpečnostní rizika plynoucí z používání centralizované databáze v tomto scénáři zmírnit a negativní dopad na základní práva a svobody subjektů údajů lze považovat za přiměřený očekávanému přínosu. Pokud jde o zásadu omezení uložení, nebyly sboru poskytnuty žádné informace, které by prokazovaly dlouhou dobu uložení. Aby bylo v tomto případě dosaženo souladu s čl. 5 odst. 1 písm. e) GDPR, měli by být správci schopni zdůvodnit, proč je plánovaná doba uchovávání pro daný účel v konkrétních případech nezbytná. Sbor doporučuje, aby správci počítali s co nejkratší dobou uložení a zároveň nabídli cestujícím možnost stanovit si upřednostňovanou dobu uložení. S ohledem na tyto skutečnosti dospěl sbor k závěru, že zpracování předpokládané ve druhém scénáři **lze v zásadě považovat za slučitelné s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR**, pokud budou zavedeny vhodné záruky.

Sbor určil záruky, které by měly být v minimálním rozsahu zavedeny v případě řešení, které se podobá druhému scénáři.

Třetí scénář zahrnuje centralizované uložení zaregistrované biometrické šablony v zašifrované podobě v rámci letiště pod kontrolou provozovatele letiště. To umožňuje identifikaci cestujících (porovnáním 1:N) při průchodu výše uvedenými letištními kontrolními stanovišti. Doba uložení je v tomto scénáři obvykle 48 hodin a údaje jsou vymazány, jakmile letadlo vzlétne.

Vzhledem k tomu, že jsou identifikační a biometrické údaje uloženy v centrální databázi, může případné narušení důvěrnosti databáze následně poskytnout přístup k celému souboru údajů a umožnit neoprávněnou nebo nezákonnou identifikaci cestujících v jiných prostředích. Centralizovaná architektura uložení údajů pod kontrolou provozovatele letiště má také za následek to, že cestující ve větší míře ztrácí kontrolu nad svými údaji. Sbor se domnívá, že podobného výsledku jako zefektivnění toku cestujících na letištích lze dosáhnout způsobem, který má méně narušující povahu, a že negativní dopad na základní práva a svobody subjektů údajů, jenž by byl důsledkem narušení důvěrnosti údajů v centralizované databázi biometrických údajů, zřejmě převažuje nad očekávaným přínosem plynoucím ze zpracování. Zpracování proto nemůže splňovat zásady nezbytnosti a přiměřenosti. Na základě těchto skutečností dospěl sbor k závěru, že zpracování předpokládané ve třetím scénáři **nemůže být slučitelné s článkem 25 GDPR**. Dále **by nebylo v souladu s čl. 5 odst. 1 písm. f) a článkem 32 GDPR**, pokud by se správce omezil na opatření popsaná v tomto scénáři.

Čtvrtý scénář zahrnuje centralizované uložení zaregistrované biometrické šablony v zašifrované podobě v cloudu pod kontrolou letecké společnosti nebo jejího poskytovatele cloudových služeb. To umožňuje identifikaci cestujících (porovnáním 1:N) při průchodu výše uvedenými letištními kontrolními stanovišti. Doba uložení může v tomto případě být tak dlouhá, po jakou má zákazník u letecké společnosti účet.

Vzhledem k tomu, že jsou identifikační a biometrické údaje uloženy v centrální databázi v cloudu, mohlo by k nim mít přístup více subjektů, případně i poskytovatelé mimo EHP. Údaje cestujících jsou při použití dešifrovány a klíče jsou pod kontrolou letecké společnosti nebo jejích zpracovatelů, což by mohlo zvýšit vystavení bezpečnostním rizikům. Tato centralizovaná architektura uložení údajů má také za následek to, že cestující ve větší míře ztrácí kontrolu nad svými údaji. Údaje by navíc mohly být

uchovávány po značně dlouhou dobu, což vystavuje údaje vyššímu riziku narušení bezpečnosti a zjevně překračuje rámec toho, co je pro účely zpracování nezbytně nutné a přiměřené, pokud nejsou přijata další opatření, která jasným způsobem rizika vznikající fyzickým osobám zmírní.

Sbor se domnívá, že podobného výsledku jako zefektivnění toku cestujících na letištích lze dosáhnout způsobem, který má méně narušující povahu, a že negativní dopad na základní práva a svobody subjektů údajů, jenž by byl důsledkem narušení důvěrnosti údajů v centralizované databázi biometrických údajů, zřejmě převažuje nad očekávaným přínosem plynoucím ze zpracování. Zpracování proto nemůže splňovat zásady nezbytnosti a přiměřenosti. Na základě těchto skutečností dospěl sbor k závěru, že zpracování předpokládané ve čtvrtém scénáři **nemůže být slučitelné s článkem 25 GDPR**. Na základě informací, které má sbor k dispozici, by rovněž **nebylo v souladu s čl. 5 odst. 1 písm. e) GDPR** a **nebylo by v souladu s čl. 5 odst. 1 písm. f) a článkem 32 GDPR,** pokud by se správce omezil na opatření popsaná v tomto scénáři.

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na článek 63 a čl. 64 odst. 2 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „**GDPR**“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na článek 10 a článek 22 jednacího řádu Evropského sboru pro ochranu osobních údajů (dále jen „**sbor**“ nebo „**EDPB**“),

vzhledem k těmto důvodům:

1) Hlavním úkolem sboru je zajistit jednotné uplatňování GDPR v celém Evropském hospodářském prostoru (dále jen „**EHP**“**)**. V čl. 64 odst. 2 GDPR se stanoví, že kterýkoli dozorový úřad, předseda sboru nebo Evropská komise mohou požádat, aby sbor posoudil jakoukoli záležitost s obecnou působností nebo s účinky ve více než jednom členském státě EHP za účelem získání stanoviska.

2) Stanovisko sboru se přijme podle čl. 64 odst. 3 GDPR ve spojení s čl. 10 odst. 2 jednacího řádu EDPB do osmi týdnů poté, co předseda a příslušný dozorový úřad rozhodli o úplnosti spisu. Rozhodnutím předsedy může být tato lhůta s ohledem na složitost dané problematiky prodloužena o dalších šest týdnů,

přijal toto stanovisko:

1 ÚVOD

1.1 Shrnutí skutečností

1. Dne 16. února 2024 požádal francouzský dozorový úřad sbor o vydání stanoviska k otázce slučitelnosti používání technologie rozpoznávání obličeje provozovateli letišť a leteckými společnostmi pro biometrické ověřování nebo identifikaci cestujících s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR[2] za účelem zefektivnění toku cestujících, a to na letištních stanovištích bezpečnostní kontroly[3], při odbavení zavazadel, při nástupu do letadla a při vstupu do haly pro cestující (s výjimkou hraničních

[1] Pokud se v tomto stanovisku hovoří o „**členských státech**“, rozumějí se tím „členské státy EHP“. Pokud se v tomto stanovisku hovoří o „Unii“ nebo „EU“, rozumí se tím „EHP“.
[2] V kontextu tohoto stanoviska se „**cestujícím**“ rozumí subjekt údajů, jehož osobní údaje jsou zpracovávány pro konkrétní účel popsaný v tomto stanovisku. V níže uvedeném znění tohoto stanoviska jsou pojmy „cestující“ a „fyzická osoba“ používány zaměnitelně.
[3] Pro účely tohoto stanoviska se „**letištními stanovišti bezpečnostní kontroly**“ rozumí bezpečnostní kontroly prováděné na odpovědnost provozovatele letiště, které musí cestující podstoupit, aby mohli se mohli přesunout z odletové haly do nástupního prostoru nebo k nástupní bráně.

kontrol a kontrol prováděných bezcelními obchody) (dále jen „**žádost**“). Francouzský dozorový úřad ke své žádosti připojil popis typických případů použití (příloha I).

2. Ve své žádosti francouzský dozorový úřad uvádí, že modely, které jsou v současné době testovány na několika letištích v EU, se v jednotlivých členských státech liší, což může nést riziko, že dozorové úřady budou uplatňovat rozdílný výklad, a riziko, že budou mít tyto modely na základní práva a svobody subjektů údajů v EU rozdílný dopad[4].

3. Sbor má za to, že pro poskytnutí odpovědi na žádost je třeba zodpovědět následující otázky:

4. **Otázka č. 1**:

1.1. Může být použití technologie rozpoznávání obličeje pro biometrické ověřování **za konkrétním účelem zefektivnění toku cestujících na letištích** (stanoviště bezpečnostní kontroly, odbavení zavazadel, nástup do letadla a vstupu do haly pro cestující) slučitelné s **čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR** v případě architektury uložení údajů, kdy je biometrická šablona každého cestujícího uchovávána **pouze v rukou fyzické osoby,** např. lokálně v jeho individuálním zařízení, které má pod svou výhradní kontrolou?

1.2. Pokud by toto zpracování bylo shledáno slučitelným s výše uvedenými ustanoveními, jaké minimální vhodné záruky by byly nutné s ohledem na články 25 a 32 GDPR?

Otázka č. 2:

2.1. Může být použití technologie rozpoznávání obličeje pro biometrické ověřování nebo identifikaci **za konkrétním účelem zefektivnění toku cestujících na letištích** (stanoviště bezpečnostní kontroly, odbavení zavazadel, nástup do letadla a vstupu do haly pro cestující) slučitelné s **čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR** v případě **centralizované** architektury uložení údajů, kdy je biometrická šablona každého cestujícího uchovávána v centrální databázi:

2.1.1. V centrální databázi na letišti, pod kontrolou provozovatele letiště, v zašifrované podobě, s klíčem / tajným heslem, které má v rukou pouze daná fyzická osoba (například ve svém mobilním telefonu), za účelem ověření?

2.1.2. Pokud by toto zpracování bylo shledáno slučitelným, jaké minimální vhodné záruky by byly nutné s ohledem na články 25 a 32 GDPR?

2.2.1. V centrální databázi na letišti, pod kontrolou provozovatele letiště, v zašifrované podobě, s klíči, které má v držení provozovatel letiště, za účelem identifikace?

2.2.2. Pokud by toto zpracování bylo shledáno slučitelným, jaké minimální vhodné záruky by byly nutné s ohledem na články 25 a 32 GDPR?

2.3.1. V cloudu, pod kontrolou letecké společnosti nebo jejího poskytovatele služeb (zpracovatele), v zašifrované podobě, s klíči, které má v držení letecká společnost nebo její poskytovatel služeb, za účelem identifikace?

[4] Žádost, s. 1.

2.3.2 Pokud by toto zpracování bylo shledáno slučitelným, jaké minimální vhodné záruky by byly nutné s ohledem na články 25 a 32 GDPR?

5. Poté, co dne 16. února 2024 francouzský dozorový úřad rozhodl o úplnosti spisu a dne 23. února 2024 předseda sboru rozhodl o úplnosti spisu, rozeslal sekretariát spis dne 23. února 2024. Předseda sboru v souladu s čl. 64 odst. 3 GDPR ve spojení s čl. 10 odst. 2 jednacího řádu sboru EDPB rozhodl prodloužit standardní lhůtu v délce osmi týdnů o dalších šest týdnů z důvodu složitosti dané záležitosti.

1.2 Přípustnost žádosti o stanovisko podle čl. 64 odst. 2 GDPR

6. V čl. 64 odst. 2 GDPR se zejména stanoví, že kterýkoli dozorový úřad může požádat, aby sbor posoudil jakoukoli záležitost s obecnou působností nebo s účinky ve více než jednom členském státě za účelem získání stanoviska.

7. Sbor se domnívá, že žádost předložená francouzským dozorovým úřadem týkající se slučitelnosti používání technologie rozpoznávání obličeje pro biometrické ověřování nebo identifikaci za konkrétním účelem zefektivnění toku cestujících na letištích se týká otázek „s účinky ve více než jednom členském státě“, protože, jak je vysvětleno v žádosti[5], v současné době se na letištích členských států zavádí několik projektů a odhaduje se, že v nadcházejících letech se míra používání této technologie zvýší. Modely, které jsou v současné době testovány různými letišti a leteckými společnostmi, se v jednotlivých členských státech značně liší, což by mohlo nést riziko, že z hlediska ochrany osobních údajů by ve více členských státech mohly mít tyto modely rozdílné dopady.

8. Sbor se rovněž domnívá, že žádost, kterou předložil francouzský dozorový úřad, má významné důsledky pro uplatňování zásad stanovených v čl. 5 odst. 1 písm. e) a f) GDPR, které se vztahují na správce podle článku 25 GDPR, jakož i požadavků, které se vztahují na správce a zpracovatele podle článku 32 GDPR. Tato žádost se proto týká „záležitosti s obecnou působností“ ve smyslu čl. 64 odst. 2 GDPR, neboť souvisí s jednotným výkladem zásad omezení uložení (čl. 5 odst. 1 písm. e) nařízení GDPR) a integrity a důvěrnosti (čl. 5 odst. 1 písm. f) GDPR) a pojmů záměrná a standardní ochrana osobních údajů (článek 25 GDPR) a zabezpečení osobních údajů (článek 32 GDPR), aby se mimo jiné zajistilo jednotné uplatňování těchto ustanovení v EHP.

9. Případné rozdílné postoje členských států k výkladu čl. 5 odst. 1 písm. e) a f) a článků 25 a 32 GDPR by zvýšily riziko, že provozovatelé letišť a letecké společnosti budou vyvíjet projekty rozpoznávání obličeje nejednotným způsobem. Vzhledem k tomu, že francouzský dozorový úřad prokázal jasnou potřebu jednotného výkladu těchto ustanovení ve vztahu k technologii rozpoznávání obličeje pro biometrické ověřování nebo identifikaci cestujících, aby se zefektivnil tok cestujících na letištích[6], má sbor za to, že žádost je v souladu s čl. 10 odst. 3 jednacího řádu EDPB odůvodněná.

10. Podle čl. 64 odst. 3 GDPR sbor EDPB nevydá stanovisko, pokud již v dané věci stanovisko vydal[7]. EDPB dosud neposkytl odpovědi na otázky vyplývající ze žádosti. Ačkoli pokyny sboru EDPB č. 3/2019 k videozařízením[8] již některé užitečné prvky související s bezpečnostními opatřeními, která by měla být uplatňována při zpracování biometrických údajů, poskytují, neřeší všechny aspekty týkající se otázek

[5] Žádost, s. 3.
[6] Žádost, s. 1–3.
[7] Ustanovení čl. 64 odst. 3 GDPR a čl. 10 odst. 4 jednacího řádu EDPB.
[8] Pokyny sboru EDPB č. 3/2019 ke zpracování osobních údajů prostřednictvím videozařízení, verze 2.0, přijaté dne 29. ledna 2020 (dále jen „**pokyny EDPB č. 3/2019 k videozařízení**m“).

vznesených v žádosti. Konkrétní pokyny k možným prvkům, které je třeba ověřit v souvislosti s centralizovaným nebo decentralizovaným uložením biometrických údajů pro identifikaci nebo ověření cestujících za účelem zefektivnění toku cestujících na letištích, a ke slučitelnosti tohoto zpracování s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR neposkytují ani dostupné pokyny sboru EDPB, včetně pokynů EDPB č. 3/2019 k videozařízení.

11. Z těchto důvodů se sbor domnívá, že žádost je přípustná a otázky v ní vznesené by měly být analyzovány ve stanovisku, které bude přijato podle čl. 64 odst. 2 GDPR.

2 OBLAST PŮSOBNOSTI A SOUVISLOSTI STANOVISKA

2.1 Oblast působnosti stanoviska

12. Toto stanovisko se týká pouze slučitelnosti používání technologie rozpoznávání obličeje pro biometrické ověřování nebo identifikaci cestujících provozovateli letišť a leteckými společnostmi za **konkrétním účelem zefektivnění toku cestujících na letištích**, a to na stanovištích bezpečnostní kontroly, při odbavení zavazadel, při nástupu do letadla a při vstupu do haly pro cestující, jak je uvedeno v žádosti, s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GPDR.

13. Pokud jde o **oblast působnosti tohoto stanoviska**, sbor objasňuje následující skutečnosti:

1) Zpracování osobních údajů v rámci hraničních kontrol a kontrol prováděných bezcelními obchody nespadá do oblasti působnosti tohoto stanoviska, neboť je provádějí jiní správci než provozovatelé letišť a letecké společnosti.

2) Používání technologie rozpoznávání obličeje, byť je založeno na scénářích popsaných níže v oddíle 3.2, pro jakékoli jiné účely (např. prosazování práva) nebo jakýmikoli jinými stranami, i když pro podobné účely, nespadá do oblasti působnosti tohoto stanoviska.

3) Toto stanovisko se zabývá pouze zpracováním osobních údajů cestujících a nevztahuje se na jiné typy subjektů údajů, jako jsou zaměstnanci provozovatelů letišť nebo leteckých společností.

4) Toto stanovisko se zabývá žádostí, kterou předložil francouzský dozorový úřad, pokud jde o slučitelnost architektury uložení biometrických šablon cestujících s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR. V tomto smyslu neobsahuje úplnou a kompletní analýzu dodržování GDPR ze strany příslušných správců a případně i jejich zpracovatelů. To je obzvláště důležité vzhledem k tomu, že tyto technologie s sebou nesou zvýšená rizika spojená se zpracováním zvláštních kategorií osobních údajů podle článku 9 GDPR. Tímto stanoviskem proto není dotčeno posouzení jiných ustanovení GDPR, pokud jde o používání technologií rozpoznávání obličeje, včetně konkrétního odvětví, na které se žádost vztahuje, ani individuální právní a technická analýza, která je založena na konkrétním plánovaném zpracování ze strany správce a okolnostech zpracování tímto správcem.

5) Toto stanovisko se nezabývá zpracováním osobních údajů dětí a nejsou jím dotčeny žádné zvláštní požadavky, které se v tomto ohledu uplatňují.

6) Tímto stanoviskem nejsou dotčeny právní požadavky a další omezení používání biometrických údajů, které vyplývají z vnitrostátních právních předpisů členských států[9].

7) Závěry tohoto stanoviska není dotčen další technologický vývoj.

8) Toto stanovisko zkoumá čtyři scénáře, jejichž specifické charakteristické rysy jsou popsány níže v oddíle 3.2. Neřeší jiné scénáře, i když se zpracování provádí pro stejné účely.

14. Francouzský dozorový úřad ve své žádosti uvedl, že zpracování biometrických údajů cestujících za účelem zefektivnění toku cestujících na letištích by vycházelo z předpokladu, že fyzické osoby s tímto zpracováním souhlasí, což by případně tvořilo právní základ podle GDPR[10]. **Do rozsahu otázek předložených sboru EDPB v žádosti však nespadá analýza použitelného právního základu, a proto se platnost souhlasu s takovým zpracováním v souladu s články 6, 7 a 9 GDPR v tomto stanovisku nezkoumá.**

15. Nicméně EDPB obecně poznamenává, že pokud by příslušní správci z tohoto právního základu chtěli vycházet, museli by získat platný výslovný souhlas[11] od fyzických osob, které chtějí tyto služby využívat. Tento výslovný souhlas by musel být svobodný, konkrétní a informovaný[12] a splnění těchto podmínek by se posuzovalo případ od případu. To mimo jiné znamená, že:

1) Fyzické osoby by musely mít možnost tento souhlas kdykoli snadno a bez újmy odvolat[13].

2) Aby byl souhlas udělen svobodně, může k takovému používání technologií využívajících biometrické údaje docházet pouze na základě dobrovolnosti, neboť fyzické osoby by měly mít možnost svobodně se rozhodnout, zda tyto služby budou využívat, či nikoliv, a to bez jakékoli újmy (například výrazně delšího zpoždění pro

[9] Například čl. 9 odst. 4 GDPR stanoví, že členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování biometrických údajů.
[10] Žádost, příloha I.
[11] Podle čl. 4 bodu 14 a čl. 9 odst. 1 GDPR, jakož i čl. 9 odst. 2 písm. a) GDPR je zakázáno zpracovávat biometrické údaje za účelem jedinečné identifikace fyzické osoby, pokud subjekt údajů neudělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v čl. 9 odst. 1 GDPR nemůže být subjektem údajů zrušen. Viz také 51., 52. a 53. bod odůvodnění GDPR.
[12] Ustanovení čl. 4 bodu 11 a článku 7 GDPR.
[13] Ustanovení čl. 7 odst. 4 GDPR, také 50. bod odůvodnění GDPR.

cestující, kteří souhlas neudělí[14]), pobídek, dodatečných nákladů nebo dalších výhod na oplátku[15].

3) Výslovný souhlas by musel být požadován také od fyzických osob, jejichž biometrické údaje jsou zpracovávány, i když se k identifikaci nebo ověření těmito prostředky nezaregistrovaly. Jinými slovy je nezbytné zajistit, aby obličeje fyzických osob, které neudělily výslovný souhlas s rozpoznáváním obličeje pro zamýšlený účel, nebyly snímány kamerami. Toho lze dosáhnout například tím, že budou vyhrazeny zvláštní koridory pro rozpoznávání obličeje a bude zajištěno vhodné značení a fyzické oddělení od toků s kontrolami, které nejsou založeny na biometrických údajích, aby bylo možné tyto koridory jasně identifikovat.

4) Aniž je dotčeno, zda by byl souhlas použitelným právním základem pro toto zpracování, uplatňují se zásady zpracování zakotvené v článku 5 nařízení GDPR, pokud jde o nezbytnost a přiměřenost, i v případě, že fyzické osoby udělily svůj výslovný souhlas s použitím svých biometrických údajů[16].

16. V žádosti je uvedeno[17], že provozovatelé letišť budou působit jako správci, pokud jde o odbavení na letištních stanovištích bezpečnostní kontroly, zatímco letecké společnosti budou působit jako správci, pokud jde o odbavení zavazadel, nástup do letadla a vstup do haly pro cestující. Sbor proto konstatuje, že do zpracování popsaného v žádosti mohou být zapojeny různé subjekty, a neposuzoval plnění rolí (společného) správce a/nebo zpracovatele ve scénářích popsaných níže v oddíle 3.2 tohoto stanoviska. V každém případě je třeba určit zapojené subjekty a jasně rozdělit jejich odpovědnosti, aby byly splněny požadavky GDPR[18].

17. Sbor dále konstatuje, že v současné době neexistuje v EU jednotný právní požadavek, který by provozovatelům letišť a leteckým společnostem ukládal povinnost identifikovat cestující a ověřovat, zda se jméno na palubním lístku cestujícího shoduje se jménem v jeho dokladu totožnosti na všech výše uvedených stanovištích kontroly[19]. Na všechny tyto požadavky se tedy vztahují vnitrostátní právní předpisy, které se mohou v jednotlivých členských státech lišit. V některých členských státech může být toto ověření vyžadováno na některých stanovištích kontroly (např. při odbavení zavazadel nebo

[14] Může to například znamenat, že systém bude kupříkladu navrhován tak, aby nevytvářel sociální tlak na cestující, kteří nechtějí udělit souhlas, tím, že zabrání tomu, aby jejich volba měla negativní dopad na ostatní cestující.

[15] Pokyny EDPB č. 5/2020 k souhlasu podle nařízení 2016/679, verze 1.1, přijaté dne 4. května 2020 (dále jen „**pokyny EDPB č. 5/2020 k souhlasu**“), body 46 a 48.

[16] Tamtéž, bod 5.

[17] Žádost, příloha I.

[18] V souladu s čl. 4 body 7 a 8, čl. 5 odst. 2, články 24, 26, 28 a 29 GDPR. Viz také Pokyny EDPB č. 7/2020 k pojmům správce a zpracovatele v GDPR, verze 2.1, přijaté dne 7. července 2021.

[19] Příslušným nařízením na úrovni EU je prováděcí nařízení Komise (EU) 2015/1998 ze dne 5. listopadu 2015, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti. Toto nařízení však neřeší kontrolu úředních dokladů totožnosti na letištních stanovištích kontroly a členské státy mají možnost upravit tuto oblast na vnitrostátní úrovni.

při nástupu do letadla), zatímco v jiných členských státech se v dnešní době žádné takové kontroly nevyžadují[20]. Existence zákonných povinností ověřovat totožnost cestujících má přímý dopad na různé postupy letišť.

18. V těchto situacích, **kdy není vyžadováno ověření totožnosti cestujících pomocí úředního dokladu totožnosti, by** proto **nemělo být prováděno žádné ověření pomocí biometrických údajů, protože by to vedlo k nadměrnému zpracování údajů, jelikož by to ve srovnání se současnou situací znamenalo zpracování dalších údajů a překračovalo by to rámec toho, co je pro příslušný účel nezbytné, což by bylo v rozporu se zásadou minimalizace údajů stanovenou v čl. 5 odst. 1 písm. c) GDPR.** Tyto skutečnosti je třeba mít na paměti při posuzování všech scénářů popsaných níže v oddíle 3.2 tohoto stanoviska.

2.2 Klíčové pojmy

19. Aby bylo možné považovat údaje za biometrické údaje podle čl. 4 bodu 14 GDPR[21], mělo by zpracování nezpracovaných údajů, jako jsou fyzické, fyziologické nebo behaviorální znaky fyzické osoby, zahrnovat měření těchto znaků, neboť biometrické údaje jsou výsledkem těchto měření[22].

20. Pomocí zobrazení obličeje fyzické osoby (fotografie nebo videa), který se nazývá biometrický „**vzorek**“, je možné získat digitální znázornění odlišných znaků tohoto obličeje (to se nazývá „**šablona**“)[23]. Sbor dále připomíná, že „biometrická] šablona je digitální znázornění jedinečných znaků, které byly získány z biometrického vzorku a mohou být uloženy v biometrické databázi“[24], která umožňuje nebo potvrzuje jedinečnou identifikaci fyzické osoby. Kromě toho „[t]ato biometrická šablona má být jedinečná a specifická pro každou fyzickou osobu a je v zásadě trvalá v čase“[25]. V procesu porovnávání, jehož cílem je identifikace nebo ověření fyzické osoby prostřednictvím rozpoznávání obličeje, se získaná biometrická šablona obvykle porovnává s uloženými objekty, aby se buď ověřila shoda, nebo aby se našla v databázi[26].

[20] To znamená, že v současné době se buď neprovádí žádné ověření, nebo se ověřuje pouze existence palubního lístku. Například na základě Protokolu o osvobození státních příslušníků Dánska, Finska, Norska a Švédska od povinnosti mít cestovní pas nebo povolení k pobytu při pobytu v jiné skandinávské zemi, než je jejich vlastní, ze dne 22. května 1954 jsou od 1. července 1954 občané Norska, Dánska, Finska a Švédska při cestování mezi těmito zeměmi osvobozeni od povinnosti mít cestovní pas nebo jiný doklad totožnosti.

[21] Viz také 51., 52. a 53. bod odůvodnění GDPR.

[22] Pokyny sboru EDPB č. 3/2019 k videozařízením, bod 74.

[23] Pokyny sboru EDPB 05/2022 k používání technologie rozpoznávání obličeje v oblasti prosazování práva, verze 2.0, přijaté dne 26. dubna 2023 (dále jen „**pokyny EDPB č. 5/2022 k rozpoznávání obličeje v oblasti prosazování práva**“), body 7 a 8.

[24] Tamtéž, bod 9.

[25] Tamtéž.

[26] Pokyny EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, body 10–11; viz také mezinárodní norma ISO/IEC 2382-37, 2022-03,
k dispozici na adrese: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [naposledy navštíveno dne 23. května 2024] (dále jen „**ISO/IEC 2382-37**“).

21. Technologie rozpoznávání obličeje může plnit dvě různé funkce – ověřovací[27] a identifikační[28]. Ačkoli jsou obě funkce odlišné, obě se opírají o zpracování biometrických údajů týkajících se identifikované nebo identifikovatelné fyzické osoby[29], a proto představují zpracování zvláštních kategorií osobních údajů podle článku 9 GDPR[30].

22. Zejména:

> Cílem **ověření** je potvrdit tvrzení o biometrických údajích porovnáním. Tomu se také říká ověření jedna ku jedné (1:1).
>
> Cílem **identifikace** je vyhledat v databázi zaregistrovaných biometrických údajů identifikátory, které lze přiřadit jedné fyzické osobě. Tomuto způsobu se také říká identifikace jedna ku mnoha (1:N).

23. V obou případech (tj. identifikace i ověření) jsou techniky rozpoznávání obličeje založeny na odhadované shodě mezi šablonami; tj. porovnávané a výchozí. Z tohoto pohledu jsou pravděpodobnostní: z porovnání se vyvodí vyšší nebo nižší pravděpodobnost, že se skutečně jedná o osobu, která má být ověřena nebo identifikována; pokud tato pravděpodobnost překročí určitou prahovou hodnotu stanovenou v systému, kterou definuje uživatel nebo tvůrce systému, bude systém předpokládat, že existuje shoda, která má být identifikována nebo ověřena[31].

[27] Sbor bere na vědomí, že připravované nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) (dosud nezveřejněné v Úředním věstníku), rovněž definuje v čl. 3 bodu 36 „biometrické ověřování“ jako „automatizované „one-to-one“ ověření totožnosti fyzických osob, včetně autentizace, porovnáním jejich biometrických údajů s dříve poskytnutými biometrickými údaji“ (viz legislativní usnesení Evropského parlamentu ze dne 13. března 2024 o návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Ustanovení čl. 3 bodu 35 aktu o umělé inteligenci definuje „biometrickou identifikaci“ jako „automatizované rozpoznávání fyzických, fyziologických, behaviorálních či psychických lidských znaků za účelem zjištění totožnosti fyzické osoby porovnáním biometrických údajů této osoby s biometrickými údaji jednotlivců, jež jsou uloženy v databázi“.

[29] ISO/IEC 2382-37.

[30] Ustanovení čl. 4 bodu 14 GDPR a pokyny EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, bod 12.

[31] Pokyny EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, bod 11. Viz také ISO/IEC 2382-37.

3 K OPODSTATNĚNOSTI ŽÁDOSTI

3.1 Obecné poznámky

24. Tento oddíl analyzuje otázky uvedené v odstavci 4 výše. V této souvislosti bude sbor u otázky č. 1 analyzovat slučitelnost s čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR a u otázky č. 2 slučitelnost s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR.

25. Za tímto účelem bude sbor analyzovat čtyři různé scénáře[32], jejichž specifické charakteristiky jsou popsány níže v oddíle 3.2.

26. Na úvod sbor připomíná, že používání biometrických údajů, a zejména technologie rozpoznávání obličeje, s sebou nese zvýšená rizika pro práva a svobody subjektů údajů. V první řadě se jedná o zpracování biometrických údajů, kterým je podle článku 9 GDPR poskytována zvláštní ochrana. Biometrické údaje především nevratně mění vztah mezi tělem a identitou, protože činí znaky lidského těla „strojově čitelnými“ a podléhajícími dalšímu použití[33]. Používání technologie rozpoznávání obličeje navíc může nést rizika spojená s falešně negativními výsledky, předpojatostí a diskriminací[34] a možné zneužití biometrických údajů by mohlo mít pro fyzické osoby závažné důsledky, jako je podvodné zneužití totožnosti nebo vydávání se za jinou osobu[35]. Je třeba rovněž poznamenat, že pokud se rozpoznávání obličeje provádí na dálku a bez aktivní účasti subjektu údajů, mohou si být fyzické osoby tohoto zpracování a souvisejících rizik ještě méně vědomy. V neposlední řadě je důležité zdůraznit, že znaky, na nichž jsou biometrické údaje založeny, lze obecně považovat za trvalé a mělo by se s nimi zacházet jako s neodvolatelnými, zejména v souvislosti s rozpoznáváním obličeje[36].

27. S ohledem na výše uvedené skutečnosti by proto správci měli před použitím těchto technologií, i kdyby byly považovány za zvláště účinné, posoudit dopad na základní práva a svobody subjektů údajů a zvážit, zda lze legitimního účelu zpracování dosáhnout méně rušivými prostředky[37].

---

[32] Čtyři scénáře analyzované sborem vycházejí z případů použití uvedených v příloze I žádosti. Francouzský dozorový úřad objasnil, že případy použití uvedené v příloze I žádosti jsou příklady uplatňování, které jsou součástí scénáře a slouží k ilustračním účelům.

[33] Stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k vývoji biometrických technologií přijaté dne 27. dubna 2012, WP193 (dále jen „**stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k biometrickým technologiím**“), s. 4. Je nutné uvést, že se toto stanovisko týká směrnice 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice o ochraně údajů“). GDPR rozšířilo rozsah zvláštních kategorií údajů a na rozdíl od směrnice o ochraně údajů stanoví, že biometrické údaje jsou zvláštní kategorií údajů (článek 9 GDPR).

[34] Pokyny k rozpoznávání obličeje, Poradní výbor Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních údajů, červen 2021, s. 15; také pokyny sboru EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, bod 27.

[35] Stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k biometrickým technologiím, s. 29.

[36] Pokyny EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, bod 104.

[37] 39. bod odůvodnění nařízení GDPR. Viz také pokyny EDPB č. 3/2019 k videozařízením, bod 73.

28. Sbor rovněž připomíná, že právo na ochranu osobních údajů není absolutním právem a mělo by být vyváženo ostatními základními právy chráněnými Listinou v souladu se zásadou proporcionality[38].

29. Ustanovení čl. 25 odst. 1 GDPR odkazuje na „zásady ochrany údajů“, které jsou uvedeny v článku 5 GDPR[39], a požaduje jejich provedení „účinným způsobem“[40]. To výslovně zahrnuje zásadu minimalizace údajů podle čl. 5 odst. 1 písm. c) GDPR[41], která vyžaduje, aby osobní údaje byly „přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány, a která uvedenou zásadu proporcionality vyjadřuje“[42]. Kromě toho čl. 25 odst. 2 GDPR upřesňuje povinnost „standardní minimalizace údajů“ tím, že stanoví, že se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti[43].

30. Článek 25 GDPR však nevyžaduje, aby správci zavedli konkrétní technická a organizační opatření, ale spíše požaduje, aby zvolená opatření a záruky byly specifické s ohledem na kontext a rizika pro práva a svobody subjektu údajů, která zpracování představuje[44]. Podobně článek 32 GDPR týkající se zabezpečení zpracování vyžaduje, aby správci a zpracovatelé provedli vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající riziku pro práva a svobody fyzických osob.

31. Důležité je, že i kdyby cestující výslovně souhlasili s použitím svých biometrických údajů za účelem zefektivnění toku cestujících na letištích, stále platí zásady zpracování zakotvené v GDPR týkající se nezbytnosti a přiměřenosti, které je třeba dodržovat[45].

---

[38] 4. bod odůvodnění nařízení GDPR. V tomto ohledu viz také rozsudek Soudního dvora ze dne 22. června 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (dále jen „věc C-439/19 *Latvijas Republikas Saeima*“), body 98, 110 a 113. Zásada proporcionality jako obecná zásada unijního práva navíc vyžaduje, aby opatření prováděná akty Unie byla vhodná pro dosažení sledovaného cíle a nepřekračovala rámec toho, co je k jeho dosažení nezbytné (viz rozsudek Soudního dvora ze dne 9. listopadu 2010, Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, ECLI:EU:C:2010:662 (dále jen „věci C-92/09 a C-93/09 *Volker und Schecke*“), bod 74 a citovaná judikatura).

[39] Pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, verze 2.0, přijaté dne 20. října 2020 (dále jen „**pokyny EDPB 4/2019 k záměrné a standardní ochraně osobních údajů**“), bod 11.

[40] Ustanovení čl. 25 odst. 1 GDPR uvádí: „S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů“. Viz pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, bod 13.

[41] V souladu s tím 39. bod odůvodnění nařízení GDPR stanoví, že osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky.

[42] Věc C-439/19 *Latvijas Republikas Saeima*, bod 98; rozsudek Soudního dvora ze dne 11. prosince 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (dále jen „věc C-708/18 *M5A-ScaraA*“), bod 48.

[43] Pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, bod 48.

[44] Pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, bod 14.

[45] Pokyny sboru EDBP č. 5/2020 k souhlasu podle nařízení 2016/679, bod 5.

32. Pokud jde o **zásadu nezbytnosti**, sbor zváží, zda je navrhované zpracování nezbytné pro dosažení sledovaného cíle a zda lze stejného cíle dosáhnout stejně účinně jinými prostředky, které méně narušují základní práva a svobody subjektu údajů[46]. Pokud jde o **zásadu přiměřenosti**, sbor posoudí, zda je negativní dopad na základní práva a svobody subjektů údajů úměrný očekávanému přínosu. Pokud je přínos relativně malý, pak takový dopad nemusí být přiměřený[47].

33. I když se sbor domnívá, že jeden z níže analyzovaných scénářů by mohl splňovat požadavky čl. 5 odst. 1 písm. e) a f) a článků 25 a 32 GDPR, je na správci, aby jejich splnění v každém případě prokázal skutkovými okolnostmi. Toto prokázání by mělo zahrnovat zvážení alternativních scénářů.

3.2 O slučitelnosti s čl. 5 odst. 1 písm. e) a f), články 25 a 32 GDPR

3.2.1 Scénář 1: uložení zaregistrované biometrické šablony pouze v rukou jednotlivce pro účely ověření

34. Tento oddíl zkoumá slučitelnost uložení biometrické šablony cestujícího pouze v rukou fyzické osoby, například v jejím individuálním zařízení[48], pod její výhradní kontrolou[49], pro účely ověření[50] (dále jen „**scénář 1**“), s čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR. Tento oddíl rovněž zkoumá vhodné záruky pro scénář 1 s ohledem na články 25 a 32 GDPR.

Popis scénáře

35. Ve scénáři 1 je zaregistrovaná biometrická šablona každého cestujícího, který s tímto zpracováním souhlasil, uložena pouze v rukou fyzické osoby, například na individuálním zařízení, které má každý cestující pod svou výhradní kontrolou. Cestující jsou ověřováni (porovnáním 1:1), když procházejí určitými stanovišti kontroly na letišti.

36. Registraci provádí provozovatel letiště, a to buď na dálku prostřednictvím aplikace provozovatele letiště[51], nebo na letištních terminálech s příslušnou úrovní ověření totožnosti (např. prostřednictvím rámce eIDAS s příslušnou úrovní ověření[52]). Tato registrace spočívá v tom, že se na zařízení cestujícího zaznamená biometrická šablona a identifikační údaje[53], které jsou nezbytné pro zpracování. Registrace se provádí pouze jednou a na určitou dobu platnosti (která se například shoduje s dobou platnosti

[46] Věc C-439/19 *Latvijas Republikas Saeima*, body 110 a 113; rozsudek Soudního dvora (velkého senátu) ze dne 4. července 2023, Meta v. Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, bod 108.
[47] Věc C-708/18 *M5A-ScaraA*, body 52–56, věci C-92/09 a C-93/09 *Volker und Schecke*, bod 87, věc C-439/19 *Latvijas Republikas Saeima*, body 98, 110, 113. Viz také stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k biometrickým technologiím, s. 8.
[48] Alternativně by si fyzická osoba mohla biometrickou šablonu vytisknout a uložit si ji v papírové podobě.
[49] Tím není dotčena celková odpovědnost správce za zpracování.
[50] Příkladem je případ použití 1 v příloze I žádosti.
[51] Sbor EDPB podotýká, že v budoucnu by se mohlo uvažovat o alternativních způsobech této registrace a že by registrace mohla být případně provedena bez aplikace konkrétního provozovatele letiště, například prostřednictvím interakce s digitální peněženkou uživatele.
[52] Rámec pro elektronickou identifikaci a služby vytvářející důvěru (dále jen „**eIDAS**“) na základě nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu.
[53] Pro účely tohoto stanoviska se identifikačními údaji rozumí údaje, jako je příjmení, jméno, datum narození atd., jejichž správnost byla ověřena na základě dokladu totožnosti nebo cestovního pasu.

cestovního pasu cestujícího). Provozovatel letiště po dokončení procesu registrace neuchovává ani údaje o totožnosti cestujícího, ani jeho biometrické údaje.

37. Pokud jde o uložení, identifikační údaje cestujícího a biometrická šablona jsou uloženy lokálně v zařízení každého cestujícího (např. v mobilní aplikaci provozovatele letiště nebo v aplikaci digitální peněženky). Zařízení pak může být použito k předávání identifikačních údajů a biometrické šablony cestujícího, případně včetně informací o letu a/nebo palubního lístku, nebo k učinění dotazu ohledně nich. Tyto informace jsou například zašifrovány pomocí klíče, který má v držení pouze provozovatel letiště, a to třeba ve formě kódu QR, který lze vytisknout na papír nebo zobrazit na displeji zařízení cestujícího. V tomto případě by cestující ukázal tento kód QR speciálním kontrolním modulům na letišti, které jsou vybaveny skenerem kódů QR a kamerou.

38. Z hlediska bezpečnosti jsou kódy QR při porovnávání dešifrovány pomocí klíče, který má v držení provozovatel letiště a který je jako jediný schopen kódy QR dešifrovat. Biometrické údaje cestujících jsou uchovávány pouze po velmi krátkou dobu a po dokončení porovnání jsou vymazány. Je třeba poznamenat, že bezpečnostní opatření týkající se uložení částečně závisí na zabezpečení zařízení cestujícího.

Posouzení EDPB

39. Scénář 1 popisuje technická a organizační opatření, která mají zajistit úroveň zabezpečení odpovídající rizikům pro subjekty údajů, jak to vyžaduje čl. 5 odst. 1 písm. f) a článek 32 GDPR. Cestující jsou ověřováni (porovnáním 1:1), když procházejí určitými stanovišti kontroly na letišti. V tomto scénáři se hlavní operace porovnávání provádí v kontextu kontrolovaného prostředí[54], do kterého jsou cestující aktivně zapojeni a mají větší kontrolu nad svými údaji. Zejména by byli kontrolováni pouze cestující, kteří s takovým zpracováním souhlasili, a protože by byli kontrolováni u vyhrazených modulů, biometrické údaje ostatních cestujících, kteří s tímto zpracováním nesouhlasili, by nebyly shromažďovány. Kromě toho mají cestující, kteří udělili souhlas, možnost zpracování kdykoli zastavit tím, že vymažou údaje ze svého zařízení.

40. Použití rozpoznávání obličeje na základě biometrické šablony uložené pouze v rukou jednotlivce, která může být například na individuálním zařízení, které má cestující pod svou výhradní kontrolou a které se používá k ověřování na konkrétních stanovištích kontroly prostřednictvím vyhrazeného rozhraní, představuje za určitých podmínek menší rizika ve srovnání s použitím biometrických údajů, kdy jsou údaje uloženy v centralizované databázi[55]. Toto lokalizované uložení, pokud je doprovázeno vhodnými zárukami[56], snižuje závažnost narušení zabezpečení osobních údajů ve srovnání s centralizovaným

[54] „Nekontrolované prostředí“ se týká používání rozpoznávání obličeje pro identifikaci bez aktivní účasti subjektů údajů, kdy se šablona každého obličeje vstupujícího do monitorovacího prostoru porovnává se šablonami z širokého průřezu populace uloženými v databázi, viz pokyny EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, bod 17.
[55] Pokyny EDPB č. 5/2022 k rozpoznávání obličeje při prosazování práva, bod 17.
[56] Jak je uvedeno níže od bodu 46.

uložením, pokud jde o počet dotčených fyzických osob, a zajišťuje, že přístup k biometrické šabloně zahrnuje aktivní zapojení subjektu údajů.

41. Kromě toho by se porovnávání mohlo provádět lokálně na letišti porovnáním biometrické šablony, například obsažené v kódu QR, s výstupem šablony vypočtené na základě biometrického vzorku zachyceného kamerou kontrolního modulu. Výsledek porovnání by byl znám pouze správci provádějícímu konkrétní kontrolu (což by mohl být buď provozovatel letiště, nebo letecká společnost v závislosti na tom, zda se kontrola provádí na letištních stanovištích kontroly bezpečnosti, při odbavení zavazadel, při nástupu do letadla a/nebo při vstupu do haly pro cestující) a pouze jím by byl použit. Kromě toho skutečnost, že informace potřebné pro porovnání (např. kód QR) musí být poskytnuty fyzickou osobou, působí jako druhý faktor[57], a posiluje tak bezpečnost ověření.

42. Pokud jde o slučitelnost s článkem 25 GDPR, a zejména o splnění požadavku minimalizace údajů, je třeba zajistit, aby zpracování splňovalo zásadu nezbytnosti. V případě scénáře 1 lze mít za to, že zvolená opatření splňují zásadu nezbytnosti ve vztahu ke sledovanému účelu (tj. zefektivnění toku cestujících), pokud správce může v závislosti na okolnostech zpracování prokázat, že neexistují alternativní řešení, která mají méně narušující povahu a která by mohla dosáhnout totožného cíle stejně účinně. Správce může být například schopen prokázat, že i když by cestující museli ukázat své zařízení, scénář 1 urychluje proces ověření ve srovnání se současnou situací, kdy je lidským faktorem kontrolováno, zda se jméno na palubním lístku shoduje s dokladem totožnosti cestujícího[58]. To však nelze prokázat, pokud se v současné době neprovádějí žádné kontroly k ověření totožnosti cestujících na základě jejich úředního dokladu totožnosti (v tomto ohledu viz bod 18 výše).

43. Provozovatel letiště navíc biometrické šablony po registraci neuchovává a doba uchovávání biometrických údajů správcem provádějícím kontrolu je velmi krátká, protože tyto údaje jsou vymazány, jakmile je porovnávání ukončeno. Opatření zvolená ve scénáři 1 tedy zjevně omezují rozsah zpracování a dobu uložení osobních údajů.

44. Pokud jde o zásadu přiměřenosti, narušující povaha tohoto zpracování může být vyvážena aktivním zapojením cestujících, protože jejich biometrické údaje by byly uloženy pouze v jejich rukou. Kromě toho, s ohledem na výše popsaná opatření a za předpokladu, že správce zavede vhodné záruky, jak to vyžaduje dané konkrétní zpracování, by provedení vhodných opatření mohlo zajistit úroveň bezpečnosti, která odpovídá riziku. V takovém případě by negativní dopad na základní práva a svobody subjektů údajů mohl být považován za přiměřený očekávanému přínosu.

45. S ohledem na výše uvedené skutečnosti proto sbor v odpovědi na otázku 1.1 dospěl k závěru, že toto zpracování **lze v zásadě považovat za slučitelné s čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR, a to za předpokladu, že budou zavedeny vhodné záruky**.

Vhodné záruky

[57] Tím se například snižuje riziko falšování totožnosti. Viz také níže uvedená záruka C.1.2.

[58] Lze také tvrdit, že biometrická kontrola může být méně náchylná k chybám než kontrola prováděná lidským faktorem.

46. V tomto typu scénáře se sbor EDPB v odpovědi na otázku 1.2 domnívá, že by měly být zavedeny alespoň tyto záruky. K dosažení stejných cílů v oblasti bezpečnosti a ochrany údajů lze použít i jiné záruky než ty, které jsou popsány v tomto stanovisku, a tyto záruky mohou být zákonné, pokud zajišťují soulad s platným právním rámcem.

47. Poznámka: jedná se o stručný a neúplný přehled možných vhodných záruk, které by měl správce zavést u řešení podobného scénáři 1. Jejich vhodnost podle článků 25 a 32 GDPR bude záviset na analýze jednotlivých případů. Všichni správci budou muset zajistit, aby provedli vlastní posouzení vlivu na ochranu osobních údajů[59] a jejich konkrétní řešení mohou vyžadovat další opatření, která nejsou zahrnuta v tomto stanovisku.

A. Obecné aspekty

A.1 Posouzení vlivu na ochranu osobních údajů

A.1.1 Provedení posouzení vlivu na ochranu osobních údajů v souladu s požadavky článku 35 GDPR vždy, když správce plánuje novou operaci zpracování, která může představovat vysoké riziko. To je pravděpodobně případ scénáře 1, protože zahrnuje zpracování biometrických údajů ve velkém rozsahu[60]. Vyhodnocení vhodnosti zavedení systému rozpoznávání obličeje, včetně jeho nezbytnosti a přiměřenosti vzhledem ke sledovaným účelům[61], v rané fázi návrhu a jeho přezkoumání v průběhu celého životního cyklu vývoje systému;

A.1.2 Konzultace s příslušným dozorovým úřadem v případě, že zpracování i přes opatření přijatá správcem ke zmírnění rizika stále představuje vysoké riziko[62].

A.2 Práva subjektů údajů a záruky, které mohou správci zavést

A.2.1 Záruky pro případy falešně negativních výsledků. Snižování rizika věkové, genderové a rasové předpojatosti „pravidelným hodnocením, zda algoritmy fungují v souladu s účely, a úpravou algoritmů tak, aby se zmírnily odhalené předsudky a zajistila se spravedlnost při zpracování“[63]. Například zavedením lidského dohledu a zásahů, aby se zmírnily případné předsudky a aby se zajistilo, že nedojde ke stigmatizaci nebo profilování cestujících;

[59] Článek 35 GDPR.
[60] Ustanovení čl. 35 odst. 3 GDPR a pokyny pracovní skupiny zřízené podle článku 29 pro posouzení vlivu na ochranu osobních údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 13. října 2017, WP248rev.01 – schválené sborem EDPB.
[61] Ustanovení čl. 35 odst. 7 písm. b) GDPR.
[62] Ustanovení čl. 36 odst. 1 GDPR.
[63] Pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, poznámka pod čarou č. 60, bod 70.

A.2.2 Zajištění, aby celý proces zpracování osobních údajů byl transparentní a aby fyzické osoby věděly a měly kontrolu nad tím, jak jsou jejich údaje zpracovávány při každé operaci zpracování[64];

A.2.3 Zajištění opatření pro dodržení zásady účelového omezení, aby údaje nebyly používány k jiným účelům, například pro účely bezpečnosti nebo výcviku;

A.2.4 Zajištění, aby nebyly pořizovány žádné fotografie nebo videozáznamy, i když nejsou zaznamenány a zpracovány, osob, které nesouhlasí s rozpoznáváním obličeje, a to prostřednictvím vhodných opatření (např. použití přiměřené hloubky ostrosti a oblasti snímání, aby se zabránilo pořizování snímků ostatních cestujících v pozadí nebo v okolí, zavedení vyhrazených front jasně označených pro rozpoznávání obličeje);

A.2.5 Pokud mohou stejné moduly používat cestující, kteří souhlasili i nesouhlasili s rozpoznáváním obličeje, nebo pokud se cestující, kteří nesouhlasili s rozpoznáváním obličeje, mohou objevit v zorném poli v době, kdy systém není používán, vyčkání před zahájením pořizování fotografií nebo videozáznamu na pozitivní reakci cestujícího, který souhlasil;

A.2.6 Možnost subjektu údajů kdykoli provést výmaz údajů, které jsou výhradně v jeho rukou (biometrická šablona[65]), jež jsou uchovávány v mobilní aplikaci nebo digitální peněžence[66];

A.2.7 Existence proveditelných alternativ nebo záložních řešení (tj. pro cestující, kteří by nesouhlasili s použitím svých biometrických údajů, pro cestující, kteří by nebyli schopni tato řešení využít, nebo pro cestující, u nichž by došlo k falešnému odmítnutí), aby bylo rovněž zajištěno, že cestující, kteří nesouhlasí, nepocítí žádnou újmu[67];

A.2.8 Případně používaná aplikace by měla být pečlivě navržena a nakonfigurována tak, aby neshromažďovala nadbytečné údaje a aby se zabránilo použití jakýchkoli sad pro vývoj softwaru třetích stran, které shromažďují údaje pro jiné účely.

A.3 Odpovědnost

[64] Pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, bod 68 a 7. bod odůvodnění GDPR.
[65] Odkazy na biometrickou šablonu v zárukách pro scénář 1 odpovídají odkazům na klíč / tajné heslo ve scénáři 2.
[66] Tato záruka se vztahuje pouze na scénář 1.
[67] Pokyny sboru EDPB č. 3/2019 k videozařízením, bod 86.

A.3.1 Posouzení, zda existují příslušné kodexy chování nebo certifikační mechanismy, které by pomohly prokázat soulad se zabezpečením zpracování podle článku 32 GDPR[68]. Ověření vhodnosti opatření pro dané zpracování. Při určování vhodných opatření mohou pomoci normy[69], osvědčené postupy a kodexy chování, které uznávají sdružení a další subjekty zastupující kategorie správců;

A.3.2 Zajištění, aby byly na zařízení uživatele provedeny základní bezpečnostní kontroly, které umožní fázi registrace, i když cestující má také podíl na ochraně svých údajů, protože jsou uloženy v jeho zařízení. Příklady takových technických kontrol a prověrek jsou uvedeny níže v oddíle C.2 „Infrastruktura a síť".

B. Organizační aspekty:

B.1 Politika a dodržování předpisů

B.1.1 Zajištění, aby byly zavedeny interní kontroly přístupu[70] s pravidly platnými pro administrátory;

B.1.2 Pokud může službu rozpoznávání obličeje poskytovat některá ze stran zapojených do zpracování, aniž by ostatní zapojené strany musely zpracovávat identifikační nebo biometrické údaje nebo oba druhy údajů, zákaz, aby tyto údaje proudily přes tyto ostatní strany. Například letecká společnost nemusí mít technický přístup k biometrickým údajům, pokud se spoléhá na společnou infrastrukturu letiště, i když tato letecká společnost vystupuje jako správce zpracování podle GDPR;

B.1.3 Vymezení zásad pro šifrování a správu klíčů[71], například pro zpracování identifikačních a biometrických údajů;

B.1.4 Zajištění souladu s kapitolou V GDPR. Například k zajištění souladu předávání údajů s předpisy, pokud správce používá při registraci vzdálenou službu, která sídlí ve třetí zemi;

B.1.5 Pokud je využíván zpracovatel, zajištění, aby byla uzavřena smlouva se zpracovatelem[72] v souladu s čl. 28 odst. 3 GDPR;

[68] Ustanovení čl. 32 odst. 3 a pokyny sboru EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, bod 10.
[69] Viz například ISO/IEC 2382-37.
[70] Pokyny sboru EDPB č. 4/2020 o používání lokalizačních údajů a nástrojů pro vysledování kontaktů v souvislosti s pandemií COVID-19, přijaté dne 21. dubna 2020 (dále jen „**pokyny EDPB č. 4/2020 k lokalizačním údajům a nástrojům pro vysledování kontaktů**"), SEK-10, s. 16.
[71] Pokyny EDPB č. 3/2019 k videozařízením, bod 89.
[72] Ustanovení čl. 28 odst. 3 GDPR.

B.1.6 Zajištění, aby byly zavedeny postupy pro řízení lidského dohledu a zásahů, zejména pro řešení problémů s falešným odmítnutím a technických problémů nebo problémů s použitelností.

B.2 Školení a testování

B.2.1.Zajištění, aby byl personál vhodným způsobem vyškolen;

B.2.2 Provedení „procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování[73]“

B.2.3 Zavedení postupu, který zajistí, že zpracování biometrické šablony cestujícího[74] pro účely ověření je technicky účinné a dostatečně přesné;

B.2.4 Zajištění, aby biometrické vzorky odebrané při registraci i na stanovišti kontroly byly dostatečně kvalitní pro spolehlivé zpracování biometrických údajů.

C. Technické aspekty:

C.1 Přístup

C.1.1 Zavedení záruk během fáze registrace, aby se zajistil zaváděcí proces registrace s ověřenou totožností. Například pro posílení posouzení totožnosti uživatelů lze zavést vícefaktorové ověřování, od jednorázových odkazů chráněných heslem pro aktivaci aplikace až po mechanismy pro odblokování místního zařízení;

C.1.2 Zavedení záruk pro řešení případů falešně pozitivních výsledků prezentačních útoků a prevence podvodů[75];

C.1.3 Zákaz jakéhokoli externího přístupu k identifikačním a biometrickým údajům[76];

C.1.4 Zajištění, aby zpracování probíhalo lokálně ve fázích registrace, předávání údajů a porovnávání. Místo porovnávání by mělo být co nejblíže zařízení jednotlivce. Povolení porovnávání šablon v rámci jednotlivých zařízení by mohlo vyžadovat interakci s poskytovateli služeb umístěnými mimo letiště a využívat veřejné síťové zdroje, což by mohlo mít dopad na dostupnost a šíření šablony mezi externí subjekty;

[73] Ustanovení čl. 32 odst. 1 písm. d) GDPR.
[74] Odkazy na biometrickou šablonu v zárukách pro scénář 1 odpovídají odkazům na klíč / tajné heslo ve scénáři 2.
[75] ENISA, Report on Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust of January 2022 (Zpráva o digitální identitě týkající se využití konceptu v oblasti samostatné identity (SSI) k budování důvěry z ledna 2022).
[76] Pokyny EDPB č. 3/2019 k videozařízením, bod 89.

C.1.5 Ověření uživatele za účelem přidání nového letu a vygenerování nového zašifrovaného kódu QR;

C.1.6 Zavedení opatření pro řešení situace, kdy cestující může ztratit přístup ke svému kódu QR.

C.2 Infrastruktura a síť

C.2.1 Podmínky aktualizace operačního systému a povolení ověření pro přístup k zařízení, aby aplikace/ digitální peněženka fungovala, včetně automatického vymazání identifikačních a biometrických údajů, pokud je operační systém zastaralý a představuje bezpečnostní riziko;

C.2.2 Izolace jednotek pro porovnávání (tj. modulů) od sítě při provozu a přijetí všech dalších nezbytných opatření k zajištění bezpečnosti;

C.2.3 Provedení porovnání biometrických údajů na zařízení cestujícího nebo v modulu (edge computing);

C.2.4 Řešení pro zmírnění bezpečnostních zranitelností jednotlivých zařízení cestujících, včetně šifrování (minimálně) biometrických a identifikačních údajů v době mimo používání;

C.2.5 Využití bezpečného úložiště (minimálně) biometrických údajů výhradně v rukou uživatele[77], například pomocí zabezpečené enklávy v chytrém telefonu;

C.2.6 Bezpečnostní záruky k zajištění fyzické bezpečnosti prostor, včetně letištního biometrického terminálu. Zajištění vysoké úrovně zabezpečení prvků architektury, které zpracovávají (např. výpočet, tok dat, přechodné nebo dlouhodobé uložení) identifikační a biometrické údaje.

C.3 Zabezpečení a správa údajů při kontrole totožnosti uživatele

C.3.1 Rozdělení údajů při předávání a uložení alespoň do tří různých skupin, jako jsou: identifikační, biometrické a letové údaje[78]. Zajištění, aby byly údaje mezi předáváním a uložením vhodně zašifrovány;

C.3.2 Zavedení technických opatření, která zajistí, že se na konkrétních stanovištích kontroly zpracovávají a ověřují pouze údaje, které lze zpracovávat zákonným způsobem;

[77] Odkazy na biometrickou šablonu v zárukách pro scénář 1 odpovídají odkazům na klíč / tajné heslo ve scénáři 2.

[78] Pokyny EDPB č. 3/2019 k videozařízením, bod 89.

C.3.3 Zajištění účinnosti výmazu údajů[79] prostřednictvím bezpečného postupu výmazu (například hlavní paměti, mezipaměti, případných záloh) a vyhodnocení, kdy by měl být výmaz údajů automatizován. Lhůty pro uložení údajů by měly být přísně vynucovány prostřednictvím automatických postupů, aniž by bylo nutné, aby jednotlivé fyzické osoby prováděly další úkony[80];

C.3.4 Zajištění pravosti a integrity údajů (například podpisu)[81];

C.3.5 Uchovávání biometrických údajů cestujících v místě registrace a na stanovišti kontroly pouze po velmi krátkou dobu a jejich výmaz, jakmile cestující projde stanovištěm kontroly;

C.3.6 Pokud se pro registraci používá aplikace, použití při vývoji aplikace bezpečnostních standardů pro bezpečnost mobilních aplikací a bezpečnostních testů prováděných třetí stranou;

C.3.7 Zajištění, aby byla během fáze registrace na letišti zavedena bezpečnostní opatření k zachování důvěrnosti a integrity biometrických údajů cestujících. Například pokud je kód QR vytištěn v kiosku, neměl by být kód QR v kiosku zobrazen, aby se zabránilo pořízení snímku škodlivým subjektem. V případě předávání údajů na krátkou vzdálenost by mělo předávání údajů probíhat za aktivní účasti uživatele a prostřednictvím kanálu zajišťujícího blízkost;

C.3.8 Údaje, které jsou výhradně v rukou fyzické osoby[82], by měly být uchovávány na bezpečném úložišti v zařízení fyzické osoby a případné zranitelnosti související s operačními systémy zařízení musí být opatřeny příslušnými bezpečnostními opatřeními. V případě tištěného kódu QR by měla být fyzická osoba upozorněna na zvláštní citlivou povahu údajů, které obsahuje, a na to, co umožňuje provádět;

C.3.9 Zajištění, aby registrace probíhala podle vhodných technik dálkového ověřování totožnosti[83].

3.2.2 Scénář 2: centralizované uložení zaregistrované biometrické šablony v zašifrované podobě na letišti a s klíčem / tajným heslem, které jsou výhradně v rukou cestujících, za účelem ověření

48. Tento oddíl zkoumá slučitelnost centralizovaného uložení biometrických šablon cestujících v centralizované databázi v zašifrované podobě a s klíčem / tajným heslem, které má v rukou výhradně cestující[84], s čl. 5 odst. 1 písm. e) a f) a s články 25 a 32 GDPR (dále jen „**scénář 2**“). Tento oddíl rovněž zkoumá vhodné záruky pro scénář 2 s ohledem na články 25 a 32 GDPR.

[79] Pokyny EDPB č. 3/2019 k videozařízením, bod 89.
[80] Pokyny EDPB č. 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů, bod 82.
[81] Pokyny EDPB č. 3/2019 k videozařízením, bod 89.
[82] Odkazy na biometrickou šablonu v zárukách pro scénář 1 odpovídají odkazům na klíč / tajné heslo ve scénáři 2.
[83] Viz ENISA, Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely (Zpráva o ověřování totožnosti na dálku: Analýza metod pro provádění ověřování totožnosti na dálku), březen 2021.
[84] Příkladem je případ použití 2 v příloze I žádosti.

Popis scénáře

49. Ve scénáři 2 se registrace provádí pouze jednou, a to pro dané období platnosti (například jeden rok po posledním letu, až do vypršení platnosti cestovního pasu), a to buď na dálku při odpovídající úrovni ověření totožnosti (např. odpovídající úroveň ověření rámce eIDAS), nebo na letištních terminálech. Registrace je řízena provozovatelem letiště a spočívá ve vygenerování identifikačních a biometrických údajů, které jsou zašifrovány klíčem / tajným heslem.

50. Databáze je uložena v prostorách letiště a je pod kontrolou provozovatele letiště. Šifrovací klíče / tajná hesla specifická pro fyzické osoby jsou uloženy pouze v zařízení této osoby (například v mobilní aplikaci provozovatele letiště). Aplikace může vygenerovat kód QR obsahující klíč / tajné heslo, které lze vytisknout na papír nebo zobrazit na obrazovce zařízení[85]. Kromě toho provozovatel letiště provádí druhou vrstvu šifrování[86] pomocí klíčů, které kontroluje provozovatel letiště.

51. Cestující jsou ověřováni (porovnáním 1:1), když procházejí určitými stanovišti kontroly na letišti. Cestující, kteří se rozhodnou projít biometrickými stanovišti kontroly, ukazují svůj kód QR speciálnímu stanovišti kontroly vybavenému čtečkou kódů QR a kamerou. Index cestujícího se odešle do databáze a vyžádá si zašifrovanou šablonu, která se stáhne a zkontroluje na místě v modulu a/nebo v zařízení uživatele. Pracovník kontroly stanoviště kontroly zná a používá pouze výsledek porovnání[87].

52. V tomto scénáři neexistují toky identifikačních a biometrických údajů mezi letišti, přičemž centralizované databáze nejsou vzájemně propojeny ani interoperabilní.

Posouzení EDPB

53. Ve scénáři 2 jsou biometrické šablony cestujících uloženy centrálně, ale v zašifrované podobě a s klíčem / tajným heslem, které mají v rukou cestující výhradně. Ve scénáři 2 jsou cestující ověřováni (porovnáním 1:1).

54. V tomto scénáři je navrhováno, že cíle zefektivnění toku cestujících (tj. zvýšení rychlosti odbavení) by mohlo být dosaženo pomocí centralizovaného systému. EDPB již dříve uvedl, že takové řešení by mohlo být považováno za proveditelnou alternativu k decentralizovanému uložení zaregistrovaných biometrických šablon[88] (jak je popsáno ve scénáři 1), pokud by existovaly objektivní potřeby a byly použity vhodné záruky (viz záruky popsané od bodu 60 níže).

55. Z hlediska bezpečnosti jsou údaje každé fyzické osoby šifrovány pomocí specifického klíče, který má k dispozici pouze daná fyzická osoba a který je pod její výhradní kontrolou. Kromě toho skutečnost, že informace potřebné pro porovnání (např. Tajné heslo / klíč) musí být poskytnuty fyzickou osobou, působí jako druhý faktor[89], a posiluje tak bezpečnost ověření. Provozovatel letiště navíc provádí druhou vrstvu šifrování pomocí klíčů, které kontroluje provozovatel letiště. Ve scénáři 2 je index

[85] Francouzský dozorový úřad dále upřesnil, že mohou existovat i jiná technická řešení pro zasílání požadovaných informací, například pomocí komunikačního protokolu krátkého dosahu.
[86] Klíč / tajné heslo (v rukou fyzické osoby) jsou samy o sobě zašifrované jiným klíčem, který má v držení provozovatel letiště.
[87] Francouzský dozorový úřad objasnil, že tato doba uložení je ilustrativní a může být považována za přijatelnou vzhledem k tomu, že klíč je v rukou jednotlivců a může být zvolen ve fázi registrace. Je však třeba poznamenat, že tato doba uložení může být změněna.
[88] Pokyny EDPB č. 3/2019 k videozařízením, bod 88.
[89] Tím se například snižuje riziko falšování totožnosti. Viz také záruka C.1.2.

fyzické osoby odeslán do centrální databáze za účelem získání biometrických údajů spojených s danou fyzickou osobou. Tyto údaje jsou poté odeslány (zašifrovány) do počítače umístěného ve stanovišti kontroly, kde jsou dešifrovány, aby bylo možné provést porovnání, a pracovník kontroly stanoviště kontroly zná a používá pouze výsledek porovnání. Za předpokladu, že klíč / tajné heslo fyzické osoby jsou uloženy v počítači umístěném na stanovišti kontroly a že do centrální databáze je odesílán pouze index cestujícího za účelem získání zašifrované biometrické šablony, lze tato bezpečnostní opatření považovat za slučitelná s čl. 5 odst. 1 písm. f) a článkem 32 GDPR.

56. Pokud jde o slučitelnost s článkem 25 GDPR, a zejména o splnění požadavku minimalizace údajů, je třeba zajistit, aby zpracování splňovalo zásadu nezbytnosti. V případě scénáře 2 lze mít za to, že zvolená opatření splňují zásadu nezbytnosti ve vztahu ke sledovanému účelu (tj. zefektivnění toku cestujících na letištích), pokud správce může v závislosti na okolnostech zpracování prokázat, že neexistují alternativní řešení, která mají méně narušující povahu a která by mohla dosáhnout totožného cíle stejně účinně. Ve scénáři 2 by cestující i tak museli ukázat své zařízení[90]. Správce může být však schopen prokázat, že scénář 2 urychluje proces ověření ve srovnání se současnou situací, kdy je lidským faktorem kontrolováno, zda se jméno na palubním lístku shoduje s dokladem totožnosti cestujícího[91], nebo ve srovnání se scénářem 1. To však nelze prokázat, pokud se v současné době neprovádějí žádné kontroly k ověření totožnosti cestujících na základě jejich úředního dokladu totožnosti (v tomto ohledu viz bod 18 výše).

57. Pokud jde o zásadu přiměřenost, narušující povaha tohoto zpracování může být vyvážena aktivním zapojením cestujících, kteří mají klíč ke svým zašifrovaným údajům, který mají výhradně pod svou kontrolou. Kromě toho se zdá, že bezpečnostní rizika spojená s uchováváním biometrických údajů cestujících v centralizované databázi a s klíčem, který je výhradně v rukou cestujících, lze zmírnit použitím vhodných záruk (viz záruky od bodu 60 níže). Proto za předpokladu, že správce zavede vhodné záruky, jak to vyžaduje dané konkrétní zpracování, lze rizika pro fyzické osoby zmírnit a negativní dopad na základní práva a svobody subjektů údajů lze považovat za přiměřený očekávanému přínosu. V každém případě by mělo být zajištěno, aby byly zpracovávány pouze údaje potřebné pro daný účel a aby byli kontrolováni pouze cestující, kteří s tím souhlasili, takže nebude hrozit, že by budou shromažďovány biometrické údaje jiných cestujících, kteří s tím nesouhlasili.

58. V žádosti je jako příklad uvedeno, že ve scénáři 2 by doba uložení zašifrovaných údajů v databázi mohla být obvykle jeden rok od posledního letu, který fyzická osoba uskutečnila, a to až do vypršení platnosti cestovního pasu. V žádosti nebyly poskytnuty žádné informace, které by tak dlouhou dobu odůvodňovaly objektivními důvody, ačkoli lze předpokládat, že se s takovou dobou uložení počítá z důvodů příhodnosti pro budoucí lety. Pokud jde o dobu uložení, měli by být správci v zájmu dosažení souladu s čl. 5 odst. 1 písm. e) GDPR v tomto případě schopni zdůvodnit, proč je tato doba uložení pro daný účel v konkrétních případech nezbytná. Sbor doporučuje správcům, aby počítali s co nejkratší dobou uložení, a to i s ohledem na cestující, kteří létají jen velmi zřídka, a aby subjektům údajů nabídli, že si mohou stanovit preferovanou dobu uložení.

[90] Francouzský dozorový úřad dále upřesnil, že mohou existovat i jiné možnosti prezentace šablony, např. vytištěné na papíře. Kromě toho EDPB uznává, že v budoucnu by se mohlo uvažovat o použití alternativní technologie, např. založené na systému komunikace v blízkém poli.

[91] Lze také tvrdit, že biometrická kontrola může být méně náchylná k chybám než kontrola prováděná lidmi.

59. S ohledem na tyto úvahy dospěl sbor v odpovědi na otázku 2.1.1 k závěru, že toto zpracování **lze v zásadě považovat za slučitelné s čl. 5 odst. 1 písm. e), čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR, pokud jsou zavedeny vhodné záruky**.

Vhodné záruky

60. V odpovědi na otázku 2.1.2 se sbor domnívá, že v tomto typu scénáře by **kromě záruk uvedených ve scénáři 1** měly být zavedeny alespoň níže uvedené záruky. K dosažení stejných cílů v oblasti bezpečnosti a ochrany údajů lze použít i jiné záruky než ty, které jsou popsány v tomto stanovisku, a tyto záruky mohou být zákonné, pokud zajišťují soulad s platnými právními rámci.

61. Poznámka: *jedná se o stručný a neúplný přehled možných vhodných záruk, které by mohl správce zavést u řešení podobného scénáři 2. Jejich vhodnost podle článků 25 a 32 GDPR bude záviset na analýze jednotlivých případů. Všichni správci budou muset zajistit, aby provedli vlastní posouzení vlivu na ochranu osobních údajů a jejich konkrétní řešení mohou vyžadovat další opatření, která nejsou zahrnuta v tomto stanovisku.*

D. Obecné aspekty

D.1 Práva subjektů údajů a záruky, které mohou správci zavést

D.1.1 Zajištění, aby měl cestující kontrolu nad dobou uložení všech svých údajů. Doba uložení by měla být omezena na dobu nezbytnou pro daný účel. Maximální doba by měla být stanovena na základě důkladné analýzy faktorů, jako je platnost dokladu totožnosti. Subjektům údajů by mělo být nabídnuto, aby si stanovily preferovanou dobu uložení, která by mohla být kratší než standardní doba uložení;

D.1.2 Možnost subjektu údajů kdykoli požádat o výmaz údajů, které jsou výhradně v jeho rukou (klíč / tajné heslo), jež jsou uchovávány v mobilní aplikaci nebo digitální peněžence[92];

D.1.3 Zajištění, aby lokalizace centrální databáze umožňovala účinný dohled ze strany příslušného dozorového úřadu.

E. Organizační aspekty:

E.1 Politika a dodržování předpisů

E.1.1 Důvěra v centrální server musí být omezená. Zajištění, aby se řízení centrálního serveru drželo jasně stanovených pravidel správy a zahrnovalo všechna nezbytná opatření pro zajištění jeho bezpečnosti[93].

[92] Tato záruka se vztahuje pouze na scénář 2.
[93] Pokyny sboru EDPB č. 4/2020 k lokalizačním údajům a nástrojům pro vysledování kontaktů, PRIV-5, s. 17.

F. <u>Technické aspekty</u>:

F.1 Přístup

F.1.1 Vedení záznamů o tom, kdo a kdy měl přístup k osobním údajům, zejména k identifikačním a biometrickým údajům;

F.2 Infrastruktura a síť

F.2.1 Zabezpečení centrální databáze vhodným způsobem, včetně zabezpečení proti útokům v oblasti dostupnosti;

F.2.2 Zajištění, aby k centrální databázi, modulům pro registraci a jednotkám pro porovnávání nebylo internetové připojení. Provoz a údržba těchto systémů (např. zálohování, přijímání opatření, monitorování atd.) se provádí lokálně v prostorách letiště.

F.3 Bezpečnost a správa údajů

F.3.1 Zavedení nejmodernějších kryptografických technik pro zabezpečení výměn mezi aplikací a centralizovaným serverem[94];

F.3.2 Uchovávání klíčů / tajných hesel fyzických osob na úrovni, kde bude použit k dešifrování (tj. v modulu), a používání indexu pouze k získání odpovídající zaregistrované biometrické šablony v centrální databázi;

F.3.3 Zajištění, aby výměna klíčů / tajných hesel mezi uživatelským zařízením a modulem chránila komunikaci před případným odposlechem nebo přenosem třetím stranám;

F.3.4 Provedení indexace biometrické šablony při uložení do centrální databáze, aby bylo možné provést ověření 1:1 a aby byla jedinečná a vztahovala se k dané fyzické osobě. Zajištění, aby index neodhaloval žádné identifikační údaje cestujícího a nebyl v korelaci se šifrovacím klíčem;

F.3.5 Ověření vhodným způsobem a zašifrování jakéhokoli přenosu mezi centrální databází a stanovišti kontroly a jejich umístění do izolovaných sítí;

F.3.6 Zamezení obousměrným vazbám mezi soubory údajů (identifikačními a biometrickými údaji a údaji o letu) a v databázi ponechání pouze relevantní jednosměrné

[94] Pokyny EDPB č. 4/2020 k lokalizačním údajům a nástrojům pro vysledování kontaktů, SEC-4, s. 16: „Mezi příklady technik, které lze použít, patří např.: symetrické a asymetrické šifrování, hashovací funkce, test soukromé příslušnosti, průnik soukromých množin, Bloomovy filtry, vyhledávání soukromých informací, homomorfní šifrování“.

vazby. Například pouze jednosměrné odkazy z indexu na identifikační údaje, z indexu na šifrované biometrické údaje a z indexu na údaje o letu;

F.3.7 Zajištění opatření pro zachování kontinuity provozu, například zavedením vhodných záložních úložných systémů;

F.3.8 Zajištění, aby modul neuchovával záznamy o šifrovaných nebo nešifrovaných šablonách.

3.2.3 Centralizované uložení zaregistrovaných biometrických šablon pro ověření

62. Tento oddíl zkoumá slučitelnost centralizovaného uložení zaregistrovaných biometrických šablon cestujících pro účely identifikace v případě, že tyto šablony nejsou zašifrovány klíčem / tajným heslem, které mají v držení pouze cestující, s čl. 5 odst. 1 písm. e) a f) a články 25 a 32 GDPR, a to ve dvou případech použití: 1) když jsou tyto šablony uloženy v databázi na letišti pod kontrolou provozovatele letiště[95] (dále jen „**scénář 3.1**“) a 2) když jsou tyto šablony uloženy v cloudu pod kontrolou letecké společnosti[96] (dále jen „**scénář 3.2**“).

63. Sbor se domnívá, že používání biometrických údajů pro účely **identifikace** ve velkých centrálních databázích zasahuje do základních práv subjektů údajů a mohlo by mít pro subjekty údajů závažné důsledky[97]. Kromě toho je třeba používání biometrických údajů zkoumat také ve vztahu k účelu, pro který jsou zpracovávány, a to s ohledem na zásady nezbytnosti a přiměřenosti[98].

3.2.3.1 Scénář 3.1: centralizované uložení v databázi na letišti pod kontrolou provozovatele letiště

Popis scénáře

64. Ve scénáři 3.1 je zaregistrovaná biometrická šablona cestujícího uložena v centrální databázi v prostorách letiště a pod kontrolou provozovatele letiště v zašifrované podobě. Údaje cestujících jsou rozděleny do tří databází, což znamená, že jejich identifikační údaje, zaregistrovaná biometrická šablona a informace o letu jsou uloženy ve třech různých databázích. Tyto údaje jsou šifrovány různými klíči, a to jak během uložení, tak během předávání údajů na servery provádějící porovnávání, kde je následně dešifruje provozovatel letiště.

65. Cestující se musí registrovat na každý let v krátkém časovém období před odletem (např. 48 hodin). Tato registrace může být provedena buď na dálku, nebo na letištních terminálech na odpovídající úrovni ověření totožnosti (např. odpovídající úroveň ověření rámce eIDAS). Alternativně může mít registrace stejnou podobu, jaká je popsána ve scénáři 1, a v takovém případě musí cestující odeslat své údaje ze svých digitálních peněženek do letištního systému ve lhůtě 48 hodin před odletem.

---

[95] Příkladem je případ použití 3A v příloze I žádosti.
[96] Příkladem je případ použití 3B v příloze I žádosti.
[97] Viz například stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k biometrickým technologiím, s. 8. Viz také bod 26 výše.
[98] 4. bod odůvodnění GDPR. Viz také stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k biometrickým technologiím, s. 8.

66. I v tomto případě se cestující dostaví ke speciálnímu kontrolnímu modulu vybavenému kamerou. Jejich biometrický vzorek je poté odeslán na centrální letištní server, který se pokusí porovnat údaje s údaji v centrální biometrické databázi. Cestující tak může být identifikován a zkontrolován, zda je skutečně registrován pro daný odlet (nebo pro nástup do letadla v případě kontroly při nástupu do letadla). V závislosti na stanovišti kontroly mohou být údaje zaslané zpět žádajícímu pracovníkovi kontroly stanoviště kontroly v případě potřeby minimalizovány, například na odpověď „ano/ne“ nebo na samotný výsledek porovnání. V tomto případě je pracovníkovi kontroly stanoviště kontroly předán pouze výsledek žádosti, který použije.

67. V tomto scénáři jsou identifikováni zejména cestující (porovnáním 1:N), kde N je počet cestujících očekávaných na letišti v časovém horizontu několika dnů. Kromě toho se biometrické porovnání provádí pouze tehdy, když se každý cestující dostaví na předem stanovená stanoviště kontroly na letišti odletu, nicméně samotné zpracování údajů se provádí na centrálním serveru připojeném k centrální databázi. Doba uložení je v tomto scénáři obvykle 48 hodin a údaje jsou vymazány, jakmile letadlo vzlétne.

Posouzení EDPB

68. Jak je uvedeno výše, zpracování biometrických údajů s sebou nese zvýšená rizika pro práva a svobody subjektů údajů[99]. Jakékoli selhání v zabezpečení údajů tak může mít obzvláště závažné důsledky pro subjekty údajů[100]. Správci jsou povinni tato rizika účinně zmírňovat. Vzhledem k tomu, že v tomto scénáři je celá architektura zcela centralizovaná, ztrácejí cestující ve větší míře kontrolu nad svými údaji. Kromě toho by se mohlo zvýšit riziko, že údaje budou nakonec zpracovávány k jiným účelům, než je kontrola toku cestujících.

69. S ohledem na zásadu a požadavky na zabezpečení (čl. 5 odst. 1 písm. f) a článek 32 GDPR) je třeba vzít v úvahu, že uložení identifikačních a biometrických údajů v centrálních, i když oddělených databázích, se může stát cenným cílem útoků a narušením důvěrnosti této databáze může být následně získán přístup k celému souboru údajů. V důsledku toho může případné narušení týkající se šablon pro rozpoznávání obličeje a souvisejících identifikačních údajů umožnit neoprávněnou nebo nezákonnou identifikaci subjektů údajů v jiných prostředích. V závislosti na metodách používaných pro biometrickou identifikaci může také ohrozit další bezpečné používání šablon pro rozpoznávání obličeje jako identifikátoru. V takovém případě nelze následky narušení zmírnit, na rozdíl od případu jiného typu údaje (např. uživatelského jména, hesla), které je možné změnit[101].

70. Navíc velké množství a kvalita identifikačních a biometrických údajů, které správce uchovává, z nich činí velmi cenný cíl pro útočníka, což z hlediska bezpečnostního rizika znamená vyšší míru pravděpodobnosti. Úniky údajů by navíc mohly mít větší dopad, protože díky tomu, že jsou údaje

[99] Viz bod 26 výše.
[100] Pokyny k rozpoznávání obličeje, Poradní výbor Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních údajů, červen 2021, s. 22;
[101] V tomto ohledu viz stanovisko pracovní skupiny zřízené podle článku 29 č. 3/2012 k biometrickým technologiím, s. 34.

uloženy na centralizovaném místě, by útočníci mohli snáze získat přístup k osobním údajům většího počtu cestujících. Případné narušení by proto mohlo vystavit velký počet subjektů údajů vysokým rizikům z hlediska závažnosti, například krádeži totožnosti ve velkém měřítku, které je velmi obtížné zmírnit.

71. Proto, pokud jde o slučitelnost s čl. 5 odst. 1 písm. f) a článkem 32 GDPR, opatření předpokládaná ve scénáři 3.1[102], s přihlédnutím k současnému stavu techniky, nepostačují k zajištění úrovně bezpečnosti odpovídající riziku. Na základě toho by zpracování podle scénáře 3.1 nebylo v souladu s čl. 5 odst. 1 písm. f) a článkem 32 GDPR, pokud by se správce omezil na tato opatření.

72. S ohledem na zásadu uvedenou v čl. 5 odst. 1 písm. e) GDPR je v tomto scénáři doba uložení biometrických údajů v centrální databázi obvykle 48 hodin. Zdá se, že toto omezení uložení výrazně snižuje rizika spojená s narušením důvěrnosti osobních údajů. Doba uložení údajů však není sama o sobě rozhodujícím faktorem pro celkovou slučitelnost uvedené architektury, neboť tyto doby uložení mohou být správci údajů měněny. Navrhovaná opatření musí v každém případě splňovat požadavky na záměrnou a standardní ochranu údajů podle článku 25 GDPR.

73. Na rozdíl od scénářů 1 a 2, kde jsou cestující ověřováni, jsou ve scénáři 3.1 cestující identifikováni (porovnáním 1:N), kde N je počet cestujících očekávaných na letišti v časovém horizontu několika dnů, kteří s tímto zpracováním souhlasili při průchodu konkrétními stanovišti kontroly na letišti. To znamená vyhledávání cestujících v centrální databázi, přičemž se zpracovává každý odebraný biometrický vzorek a kontroluje se, zda se shoduje s osobou, kterou systém zná. Na rozdíl od scénáře 2 nemá cestující ve scénáři 3.1 klíče pouze ve svých rukou. V tomto scénáři mají tedy cestující nad svými biometrickými údaji podstatně menší kontrolu. Proto toto zpracování, jak je navrženo v rámci scénáře 3.1, nemůže být slučitelné s požadavky na záměrnou a standardní ochranu údajů podle článku 25 GDPR.

74. S ohledem na článek 25 GDPR by správci měli zvážit typy, kategorie a úroveň podrobnosti osobních údajů potřebných pro účely zpracování[103]. Jejich záměrná ochrana údajů by měla zohlednit zvýšená rizika pro zásady minimalizace údajů, integrity a důvěrnosti a omezení uložení při shromažďování velkého množství podrobných osobních údajů a porovnat je se snížením rizik při shromažďování menšího množství a/nebo méně podrobných informací o subjektech údajů. Standardní ochrana údajů by v žádném případě neměla zahrnovat shromažďování osobních údajů, které nejsou nezbytné pro konkrétní účel zpracování. Jinými slovy, pokud jsou některé kategorie osobních údajů nadbytečné nebo pokud nejsou podrobné údaje potřebné, protože postačují méně podrobné údaje, neměly by být shromažďovány žádné nadbytečné osobní údaje. Pokud by v tomto případě bylo možné dosáhnout stejného cíle jiným způsobem zpracování, který je k dispozici podle podmínek popsaných ve scénáři 3.1, není nutné použít technologii rozpoznávání obličeje.

75. Pokud jde o článek 25 GDPR, klíčovým prvkem záměrné a standardní ochrany údajů je autonomie subjektu údajů. Subjekt údajů by měl mít zejména co nejvyšší míru autonomie při určování způsobu použití svých osobních údajů, jakož i rozsahu a podmínek tohoto použití nebo zpracování[104]. V případě

[102] Jak je popsáno v bodech 64–67 výše.

[103] Pokyny EDPB č. 4/2019 týkající záměrné a standardní ochrany osobních údajů, bod 49.

[104] Pokyny EDPB č. 4/2019 týkající se záměrné a standardní ochrany osobních údajů, bod 70. V 7. bodě odůvodnění nařízení GDPR se dále upřesňuje, že „[f]yzické osoby by měly mít možnost kontrolovat své vlastní osobní údaje“.

scénáře 1 by subjekt údajů měl autonomii a kontrolu nad používáním, zveřejňováním a výmazem svých biometrických šablon a v případě scénáře 2 by si subjekt údajů zachoval určitou kontrolu nad zveřejňováním svých biometrických šablon, protože by měl k dispozici šifrovací klíč / tajné heslo. Ve scénáři 3.1 je však subjekt údajů plně závislý na rozhodnutích správce, pokud jde o zpracování jeho biometrických údajů, a nemá tedy žádnou přímou kontrolu nad použitím své biometrické šablony.

76. Pokud jde o slučitelnost s článkem 25 GDPR, a zejména o splnění požadavku minimalizace údajů, nemůže zpracování předpokládané ve scénáři 3.1 splňovat zásadu nezbytnosti. Sbor se domnívá, že podobného výsledku, který by zefektivnil tok cestujících na letištích, lze dosáhnout způsobem, který méně narušuje soukromí. Toho lze například dosáhnout i bez použití biometrických údajů (i když pak by uživatelé zažívali opačnou situaci, protože by jim mohlo trvat déle, než by ukázali palubní lístek a případně úřední doklady totožnosti). Navíc jiná řešení, zejména ta, která se spoléhají na uložení biometrických údajů do místní peněženky v zařízení fyzické osoby, nebo ta, která vyžadují šifrování údajů pomocí specifického klíče uloženého v zařízení jednotlivce, umožňují dosáhnout cílů způsobem, který méně narušuje soukromí.

77. Pokud jde o zásadu přiměřenosti, zpracování předpokládané ve scénáři 3.1 by představovalo rizika pro práva subjektů údajů, která by vzhledem k aktuálnímu stavu nebylo možné zmírnit zamýšlenými opatřeními. Riziko negativního dopadu na základní práva a svobody subjektů údajů, které by mohlo vzniknout v důsledku narušení bezpečnosti údajů v centralizované databázi biometrických údajů velkého počtu fyzických osob, tedy zjevně převažuje nad očekávaným přínosem plynoucím ze zpracování, neboť tento přínos je poměrně malý, tj. mírné zvýšení pohodlí a rychlosti kontrol. Proto nemůže odůvodnit vysoce narušující povahu těchto opatření pro základní práva a svobody fyzických osob a zpracování předpokládané ve scénáři 3.1 nesplňuje zásadu přiměřenosti.

78. S ohledem na tyto skutečnosti dospěl sbor v odpovědi na otázku 2.2.1 k závěru, že pokud je zpracování prováděno za konkrétním účelem zefektivnění toku cestujících na letištích, zpracování předpokládané ve scénáři 3.1:

- **nemůže být v souladu s článkem 25 GDPR**;
- **by nebylo v souladu s čl. 5 odst. 1 písm. f) a článkem 32 GDPR**, pokud by se správce omezil na opatření popsaná ve scénáři 3.1.

3.2.3.2 Scénář 3,2: centralizované uložení v cloudu, pod kontrolou letecké společnosti

Popis scénáře

79. Ve scénáři 3.2 je biometrická šablona cestujícího uložena v cloudu pod kontrolou letecké společnosti nebo jejího poskytovatele cloudových služeb (zpracovatele údajů). V žádosti je uvedeno, že poskytovatel cloudových služeb by se měl nacházet v EHP[105]. V tomto případě jsou údaje cestujících zašifrovány, ale při použití (například při provádění operací porovnávání) jsou dešifrovány a klíče má pod kontrolou letecká společnost nebo její cloudový zpracovatel. Biometrické údaje cestujících se používají k identifikaci cestujících (porovnáním 1:N), kde N je potenciálně počet až všech zákazníků letecké společnosti[106].

80. Podobně jako v případě scénářů 1, 2 a 3.1 se i zde musí cestující nejprve zaregistrovat. Ve scénáři 3.2 je však registrace cestujících provedena jednou, a to na celou dobu, kdy má zákazník u letecké společnosti účet. Registrace se provádí buď na dálku při odpovídající úrovni ověření totožnosti (např. odpovídající úroveň ověření dle rámce eIDAS), nebo na letištních terminálech. Biometrické porovnání se provádí pouze tehdy, když se cestující dostaví na předem stanovená stanoviště kontroly na letišti, nicméně samotné zpracování údajů probíhá v cloudu.

81. Na letišti procházejí cestující speciálními kontrolními moduly vybavenými kamerou. Biometrické údaje cestujících jsou prostřednictvím žádosti odeslány na cloudový server letecké společnosti, kde se provede porovnání těchto údajů s centrální databází. Cestující tak může být identifikován a zkontrolován, zda je skutečně registrován pro daný odlet (nebo pro nástup do letadla v případě kontroly při nástupu do letadla).

82. Výsledky porovnávání lze potenciálně zpřístupnit více provozovatelům letišť, pokud má letecká společnost vyhrazený terminál nebo přístup ke společné infrastruktuře informačního systému letiště. V závislosti na stanovišti kontroly mohou být údaje zaslané zpět žádajícímu pracovníkovi kontroly stanoviště kontroly v případě potřeby minimalizovány, například na odpověď „ano/ne“ nebo na samotný výsledek porovnání. V tomto případě je pracovníkovi kontroly stanoviště kontroly znám pouze výsledek žádosti, který použije.

83. Doba uložení šablony je stanovena leteckou společností a může trvat tak dlouho, dokud má zákazník u letecké společnosti účet.

Posouzení EDPB

84. Připomínky, které již sbor vyjádřil v souvislosti se scénářem 3.1[107], platí i pro tento scénář.

---

[105] Francouzský dozorový úřad upřesnil, že se jedná o příklad, a že lze uvažovat i o poskytovatelích cloudových služeb, kteří se nenacházejí v EHP. Kromě toho lze uvažovat i o jiných řešeních uložení (např. bez využití cloudu).
[106] Francouzský dozorový úřad vysvětlil, že se jedná o příklad, a že existuje řešení, kdy se biometrické údaje předávají pokaždé před letem.
[107] Body 68–77 výše.

85. Pokud jde o zásadu a požadavky na zabezpečení (čl. 5 odst. 1 písm. f) a článek 32 GDPR), zpracování ve scénáři 3.2 probíhá v cloudu a k těmto údajům by mohlo mít přístup více subjektů, případně i poskytovatelé mimo EHP, i když jsou údaje uchovávány v EHP[108]. Tato architektura s sebou nese potenciální rizika související s předáváním osobních údajů do třetích zemí. Kromě toho, ačkoli jsou údaje cestujících zašifrovány, jsou při použití (tj. při provádění operace párování) dešifrovány, přičemž klíče jsou pod kontrolou letecké společnosti nebo jejího cloudového zpracovatele. Toto uložení může vést k dalšímu zvýšení vystavení bezpečnostním rizikům.

86. Proto, pokud jde o slučitelnost s čl. 5 odst. 1 písm. f) a článkem 32 GDPR, opatření předpokládaná ve scénáři 3.2[109], s přihlédnutím k současnému stavu techniky nepostačují k zajištění úrovně bezpečnosti odpovídající riziku. Na základě toho by zpracování podle scénáře 3.2 nebylo v souladu s čl. 5 odst. 1 písm. f) a článkem 32 GDPR, pokud by se správce omezil na tato opatření.

87. Kromě toho by podle scénáře 3.2[110] mohly být údaje uloženy po značně dlouhou dobu (tj. potenciálně po dobu, po kterou má subjekt údajů u letecké společnosti účet). Tato doba uložení vystavuje údaje vyššímu riziku narušení jejich důvěrnosti a integrity a zjevně přesahuje rámec toho, co je pro účely zpracování nezbytně nutné a přiměřené. Sbor konstatuje, že doba uložení údajů není sama o sobě rozhodujícím faktorem pro celkovou slučitelnost uvedené architektury s GDPR, neboť může být ze strany správců údajů změněna. Na základě informací, které má sbor k dispozici a které jsou obsaženy v popisu scénáře 3.2, však neexistuje dostatečné odůvodnění pro tak dlouhou dobu uložení a nejsou zřejmá žádná opatření ke zmírnění rizik pro jednotlivce. Na základě toho by navrhovaná doba uložení nebyla omezena na nezbytnou dobu v souladu se zásadou omezení uložení podle čl. 5 odst. 1 písm. e) GDPR.

88. Opatření navrhovaná ve scénáři 3.2 v žádném případě nemohou splnit požadavky na záměrnou a standardní ochranu údajů podle článku 25 GDPR. Ve scénáři 3.2 jsou biometrické šablony cestujícího uloženy v cloudu pod kontrolou letecké společnosti nebo jejího poskytovatele cloudových služeb (zpracovatele údajů). Jak je popsáno výše, k těmto údajům by mohlo mít přístup více subjektů. Biometrické údaje cestujících se navíc používají k identifikaci cestujících (porovnáním 1:N), kde N je potenciálně počet až všech uživatelů/zákazníků letecké společnosti. Tato metoda spočívá ve vyhledání osoby ve skupině osob v centrální databázi, a to tak, že se zpracuje každý zachycený obličej a ověří se, zda odpovídá osobě, kterou systém zná. Na rozdíl od scénáře 3.1 lze ve scénáři 3.2 provést srovnání v mnohem větším rozsahu, protože kritériem je zde počet všech zákazníků letecké společnosti, zatímco scénář 3.1 zahrnoval pouze počet cestujících očekávaných v časovém horizontu několika dnů.

89. Pokud jde o slučitelnost s článkem 25 GDPR, a zejména o splnění požadavku minimalizace údajů, nemůže zpracování předpokládané ve scénáři 3.2 dále splňovat zásadu nezbytnosti. Sbor se domnívá, že podobného výsledku, který by zefektivnil tok cestujících na letištích, by bylo možné dosáhnout jinými, opatřeními, které mají méně narušující povahu, například bez použití biometrických údajů, ačkoli uživatelé by se pak octli v opačné situaci, protože předložení dokladu totožnosti a palubního lístku by mohlo trvat delší dobu. Navíc jiná řešení, zejména ta, která se spoléhají na uložení

[108] EDPB 2022 Coordinated Enforcement Action on the use of cloud-based services by the public sector (Koordinovaná donucovací opatření sboru EDPB z roku2022 týkající se využívání cloudových služeb veřejným sektorem) ze dne 17. ledna 2023, s. 19.
[109] Viz body 79–83 výše.
[110] Viz bod 83 výše.

biometrických údajů do místní peněženky v zařízení fyzické osoby, nebo ta, která vyžadují šifrování údajů pomocí specifického klíče uloženého v zařízení jednotlivce, umožňují správci dosáhnout cílů způsobem, který méně narušuje soukromí.

90. Pokud jde o zásadu přiměřenosti, zpracování předpokládané ve scénáři 3.2 by představovalo rizika pro práva subjektů údajů, která by nebylo možné zmírnit zamýšlenými opatřeními. Negativní dopad na základní práva a svobody subjektů údajů, který by mohlo vzniknout v důsledku narušení bezpečnosti údajů v centralizované databázi biometrických údajů velkého počtu fyzických osob uložených na cloudu, tedy zjevně převažuje nad očekávaným přínosem plynoucím ze zpracování, neboť tento přínos je poměrně malý, tj. mírné zvýšení pohodlí a rychlosti kontrol. Proto nemůže odůvodnit vysoce narušující povahu těchto opatření pro základní práva a svobody fyzických osob a zpracování předpokládané ve scénáři 3.2 nelze považovat za přiměřené.

91. S ohledem na tyto skutečnosti dospěl sbor v odpovědi na otázku 2.3.1 k závěru, že pokud je zpracování prováděno za konkrétním účelem zefektivnění toku cestujících na letištích, zpracování předpokládané ve scénáři 3.2:

- **nemůže být v souladu s článkem 25 GDPR**;
- **by nebylo v souladu s čl. 5 odst. 1 písm. f) a článkem 32 GDPR**, pokud by se správce omezil na opatření popsaná ve scénáři 3.2;
- **by nebylo v souladu s čl. 5 odst. 1 písm. e) GDPR**, neboť na základě informací, které má sbor k dispozici, není doba uložení údajů předpokládaná ve scénáři 3.2 dostatečně odůvodněná. Aby byla dodržena zásada omezení uložení podle čl. 5 odst. 1 písm. e) nařízení GDPR, musel by správce prokázat, že osobní údaje nejsou uchovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány.

4 ZÁVĚR

92. Pokud jde o otázku 1.1, na základě žádosti o stanovisko francouzského dozorového úřadu ve vztahu k požadavkům čl. 5 odst. 1 písm. f) a článků 25 a 32 GDPR a na základě výše uvedené analýzy dospěl sbor k závěru, že:

93. použití technologie rozpoznávání obličeje pro biometrické ověřování za konkrétním účelem zefektivnění toku cestujících na letištích (stanoviště bezpečnostní kontroly, odbavení zavazadel, nástup do letadla a vstupu do haly pro cestující) by mohlo být v zásadě považováno za slučitelné se zásadami integrity a důvěrnosti podle čl. 5 odst. 1 písm. f) a článků 25 a 32 GDPR v případě architektury uložení, kdy je zaregistrovaná biometrická šablona každého cestujícího uložena lokálně na jeho individuálním zařízení a pod jeho výhradní kontrolou, pokud podléhá vhodným zárukám popsaným v bodě 46 a dále výše.

94. Pokud jde o otázku 2.1.1, na základě žádosti o stanovisko francouzského dozorového úřadu ve vztahu k požadavkům čl. 5 odst. 1 písm. e) a f) a článků 25 a 32 GDPR a na základě výše uvedené analýzy dospěl sbor k závěru, že:

95. použití technologie rozpoznávání obličeje pro biometrické ověřování za konkrétním účelem zefektivnění toku cestujících na letištích (stanoviště bezpečnostní kontroly, odbavení zavazadel, nástup do letadla a vstupu do haly pro cestující) by mohlo být v zásadě považováno za slučitelné se zásadou omezení uložení podle čl. 5 odst. 1 písm. e) a zásadami integrity a důvěrnosti podle čl. 5 odst. 1 písm. f) a články 25 a 32 GDPR v případě architektury centralizovaného ukládání, kdy je

zaregistrovaná biometrická šablona každého cestujícího uložena v centrální databázi na letišti pod kontrolou provozovatele letiště, a to v zašifrované podobě s klíčem / tajným heslem, které má v rukou výhradně daná fyzická osoba, pokud podléhá vhodným zárukám popsaným v bodě 60 a dále výše.

96. Pokud jde o otázku 2.2.1, na základě žádosti o stanovisko francouzského dozorového úřadu ve vztahu k požadavkům čl. 5 odst. 1 písm. e) a f) a článků 25 a 32 GDPR a na základě výše uvedené analýzy dospěl sbor k závěru, že:

97. použití technologie rozpoznávání obličeje pro biometrické ověřování za konkrétním účelem zefektivnění toku cestujících na letištích (stanoviště bezpečnostní kontroly, odbavení zavazadel, nástup do letadla a vstupu do haly pro cestující) v případě architektury centralizovaného uložení, kdy zaregistrované biometrické šablony cestujících nejsou zašifrovány klíčem / tajným heslem, které má každý cestující výhradně v rukou, a kdy jsou tyto šablony uloženy v databázi v rámci letiště (pod kontrolou provozovatele letiště), nemůže být slučitelné s článkem 25 GDPR. Toto zpracování by rovněž nebylo v souladu se zásadami integrity a důvěrnosti podle čl. 5 odst. 1 písm. f) a článku 32 GDPR, pokud by se správce omezil na opatření popsaná ve scénáři 3.1.

98. Pokud jde o otázku 2.3.1, na základě žádosti o stanovisko francouzského dozorového úřadu ve vztahu k požadavkům čl. 5 odst. 1 písm. e) a f) a článků 25 a 32 GDPR a na základě výše uvedené analýzy dospěl sbor k závěru, že:

99. použití technologie rozpoznávání obličeje pro biometrické ověřování za konkrétním účelem zefektivnění toku cestujících na letištích (stanoviště bezpečnostní kontroly, odbavení zavazadel, nástup do letadla a vstupu do haly pro cestující) v případě architektury centralizovaného uložení, kdy zaregistrované biometrické šablony cestujících nejsou zašifrovány klíčem / tajným heslem, které má každý cestující výhradně v rukou, a kdy jsou tyto šablony uloženy na cloudu (pod kontrolou letecké společnosti), nemůže být slučitelné s článkem 25 GDPR. Toto zpracování by rovněž nebylo v souladu se zásadami integrity a důvěrnosti podle čl. 5 odst. 1 písm. f) a článku 32 GDPR, pokud by se správce omezil na opatření popsaná ve scénáři 3.2. Na základě popisu scénáře 3.2 a informací, které má sbor k dispozici, by zpracování nebylo v souladu se zásadou omezení uložení podle čl. 5 odst. 1 písm. e) GDPR.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Anu Talus)