d

Opinia Rady (art. 64)

Opinia 11/2024 w sprawie wykorzystywania rozpoznawania twarzy do usprawnienia przepływu pasażerów w portach lotniczych (zgodność z art. 5 ust. 1 lit. e) i f), art. 25 i art. 32 RODO)

Wersja 1.1

przyjęta 23 maja 2024 r.

Przyjęto

Wersja 1.1	28 maja 2024 r.	Poprawka gramatyczna w streszczeniu (s. 3 i 4) oraz w pkt 77 i 90 opinii
Wersja 1.0	23 maja 2024 r.	Przyjęcie opinii

Streszczenie

Francuski organ nadzorczy zwrócił się do Europejskiej Rady Ochrony Danych o wydanie opinii w sprawie wykorzystywania technologii rozpoznawania twarzy przez operatorów portów lotniczych i przedsiębiorstwa lotnicze do uwierzytelniania lub identyfikacji pasażerów za pomocą danych biometrycznych w celu usprawnienia przepływu pasażerów w portach lotniczych.

Na wstępie EROD przypomina, że wykorzystywanie danych biometrycznych, a w szczególności technologii rozpoznawania twarzy, pociąga za sobą zwiększone ryzyko dla praw i wolności osób, których dane dotyczą. Odnosi się to do przetwarzania danych biometrycznych, które jest objęte szczególną ochroną na mocy art. 9 RODO. Przed zastosowaniem takich technologii, nawet gdyby uznano je za szczególnie skuteczne, administratorzy powinni ocenić wpływ na podstawowe prawa i wolności osób, których dane dotyczą, oraz rozważyć zastosowanie mniej inwazyjnych środków do osiągnięcia prawnie uzasadnionego celu przetwarzania.

Zakres niniejszej opinii, zgodnie z wnioskiem, ogranicza się do zgodności przetwarzania z **art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO** w **konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych** w czterech konkretnych punktach kontroli, a mianowicie w punktach kontroli bezpieczeństwa, przy nadawaniu bagażu, podczas wchodzenia na pokład oraz przy wejściu do poczekalni dla pasażerów. Opinia ta nie zawiera pełnej i całościowej analizy przestrzegania RODO przez administratorów i przez ich ewentualne podmioty przetwarzające we wszystkich sytuacjach. W związku z tym opinia ta pozostaje bez uszczerbku dla indywidualnej analizy prawnej i technicznej opartej na konkretnym planowanym przetwarzaniu przez administratora i jego okolicznościach. Ponadto analiza mającej zastosowanie podstawy prawnej nie wchodzi w zakres pytań przedłożonych EROD we wniosku, w związku z czym ważność zgody na takie przetwarzanie zgodnie z art. 6, 7 i 9 RODO nie została zbadana w niniejszej opinii. Co więcej, opinia pozostaje bez uszczerbku dla ograniczeń w wykorzystywaniu danych biometrycznych określonych w prawie państwa członkowskiego.

W swojej opinii EROD ocenia zgodność przetwarzania z wyżej wymienionymi przepisami RODO w kontekście **czterech konkretnych scenariuszy**.

Pierwszy scenariusz dotyczy przechowywania zarejestrowanego wzorca biometrycznego przez osobę fizyczną, na przykład na jej urządzeniu osobistym, pod jej wyłączną kontrolą w celu uwierzytelnienia (porównanie 1:1) pasażera podczas przechodzenia przez wyżej wymienione punkty kontroli w porcie lotniczym.

EROD stwierdza, że można uznać, iż wybrane środki są zgodne z zasadą konieczności, jeżeli administrator jest w stanie wykazać, że nie istnieją mniej inwazyjne rozwiązania alternatywne, które mogłyby przyczynić się do równie skutecznego osiągnięcia tego samego celu. Ponadto inwazyjny charakter przetwarzania można zrównoważyć aktywnym zaangażowaniem pasażerów, ponieważ ich wzorzec biometryczny jest przechowywany wyłącznie przez nich, na przykład na ich urządzeniu osobistym, pod ich wyłączną kontrolą, a ich dane są usuwane od razu po zakończeniu dopasowania. Na tej podstawie EROD stwierdza, że przetwarzanie przewidziane w pierwszym scenariuszu **można uznać za zasadniczo zgodne z art. 5 ust. 1 lit. f) oraz art. 25 i 32 RODO**, pod warunkiem wdrożenia odpowiednich zabezpieczeń.

EROD określiła zabezpieczenia, które należy wdrożyć jako minimum w odniesieniu do rozwiązania zbliżonego do pierwszego scenariusza.

Drugi scenariusz zakłada scentralizowane przechowywanie zarejestrowanego wzorca biometrycznego w porcie lotniczym w formie zaszyfrowanej, do której klucz dostępu posiada jedynie pasażer. Umożliwia to uwierzytelnianie pasażerów (porównanie 1:1) podczas przechodzenia przez wyżej wymienione punkty kontroli w porcie lotniczym. Wzorzec może pozostać zarejestrowany przez określony czas, na przykład do jednego roku po odbyciu ostatniego lotu, do daty upływu ważności paszportu.

EROD stwierdza, że można uznać, iż przetwarzanie takie jest zgodne z zasadą konieczności, jeżeli administrator jest w stanie wykazać, że nie istnieją mniej inwazyjne rozwiązania alternatywne, które mogłyby przyczynić się do równie skutecznego osiągnięcia tego samego celu. Ponadto inwazyjny charakter przetwarzania można zrównoważyć aktywnym zaangażowaniem pasażera, ponieważ to pasażer posiada pod swoją wyłączną kontrolą klucz dostępu do swoich zaszyfrowanych danych biometrycznych. Zakładając, że administrator wdroży odpowiednie zabezpieczenia, ryzyko dla bezpieczeństwa wynikające z korzystania ze scentralizowanej bazy danych w tym scenariuszu można by ograniczyć, a negatywny wpływ na podstawowe prawa i wolności osób, których dane dotyczą, można uznać za proporcjonalny do spodziewanych korzyści. Jeżeli chodzi o zasadę ograniczenia przechowywania, nie przekazano EROD żadnych informacji uzasadniających długi okres przechowywania. Aby w tym scenariuszu osiągnąć zgodność z art. 5 ust. 1 lit. e) RODO, administratorzy powinni być w stanie uzasadnić, dlaczego przewidywany okres przechowywania jest niezbędny do realizacji danego celu w konkretnych przypadkach. EROD zaleca, aby administratorzy zaplanowali możliwie najkrótszy okres przechowywania, a jednocześnie zaoferowali pasażerom możliwość ustalenia preferowanego okresu przechowywania. Na tej podstawie EROD stwierdza, że przetwarzanie przewidziane w scenariuszu 2 **można uznać za zasadniczo zgodne z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO**, pod warunkiem wdrożenia odpowiednich zabezpieczeń.

EROD określiła minimalne zabezpieczenia, które należy wdrożyć w przypadku stosowania rozwiązania zbliżonego do drugiego scenariusza.

Trzeci scenariusz zakłada scentralizowane przechowywanie zarejestrowanego wzorca biometrycznego w formie zaszyfrowanej w porcie lotniczym pod kontrolą operatora portu lotniczego. Umożliwia to identyfikację pasażerów (porównanie 1:N) podczas przechodzenia przez wyżej wymienione punkty kontroli w porcie lotniczym. Okres przechowywania w tym scenariuszu wynosi zazwyczaj 48 godzin, a dane są usuwane po odlocie samolotu.

Ponieważ dane identyfikacyjne i dane biometryczne są przechowywane w centralnej bazie danych, naruszenie poufności bazy danych może skutkować dostępem do całego zbioru danych i może umożliwić nieupoważnioną lub niezgodną z prawem identyfikację pasażerów w innych środowiskach. Scentralizowana architektura przechowywania danych pod kontrolą operatora portu lotniczego skutkuje również tym, że pasażer w większym stopniu traci kontrolę nad swoimi danymi. EROD uważa, że podobny rezultat w postaci usprawnienia przepływu pasażerów w portach lotniczych można osiągnąć w mniej inwazyjny sposób, a negatywny wpływ ewentualnego naruszenia ochrony danych w scentralizowanej bazie danych biometrycznych na podstawowe prawa i wolności osób, których dane dotyczą, wydaje się przeważać nad spodziewaną korzyścią wynikającą z przetwarzania danych. W związku z tym przetwarzanie to nie jest zgodne z zasadami konieczności i proporcjonalności. Na tej podstawie EROD stwierdza, że przetwarzanie przewidziane w trzecim scenariuszu **nie może być zgodne z art. 25 RODO**. **Nie byłoby ono również zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO**, gdyby administrator ograniczył się do środków opisanych w tym scenariuszu.

Czwarty scenariusz dotyczy scentralizowanego przechowywania zarejestrowanego wzorca biometrycznego w formie zaszyfrowanej w chmurze pod kontrolą przedsiębiorstwa lotniczego lub jego

dostawcy usług w chmurze. Umożliwia to identyfikację pasażerów (porównanie 1:N) podczas przechodzenia przez wyżej wymienione punkty kontroli w porcie lotniczym. Okres przechowywania w tym scenariuszu może potencjalnie trwać tak długo, jak długo klient posiada konto w przedsiębiorstwie lotniczym.

Ponieważ dane identyfikacyjne i dane biometryczne są przechowywane w centralnej bazie danych w chmurze, dostęp do tych danych może mieć wiele podmiotów, w tym ewentualnie dostawcy spoza EOG. Dane pasażera są odszyfrowywane podczas ich użycia, a klucze znajdują się pod kontrolą przedsiębiorstwa lotniczego lub jego podmiotów przetwarzających, co może zwiększyć obszar narażenia na zagrożenia w zakresie bezpieczeństwa. Taka scentralizowana architektura przechowywania danych skutkuje również tym, że pasażer w większym stopniu traci kontrolę nad swoimi danymi. Dane mogą być również przechowywane przez długi okres, co naraża dane na większe ryzyko naruszenia bezpieczeństwa i wydaje się wykraczać poza to, co jest absolutnie niezbędne i proporcjonalne do celów przetwarzania, chyba że zostaną podjęte dalsze oczywiste środki w celu ograniczenia ryzyka dla osób fizycznych.

EROD uważa, że podobny rezultat w postaci usprawnienia przepływu pasażerów w portach lotniczych można osiągnąć w mniej inwazyjny sposób, a negatywny wpływ ewentualnego naruszenia ochrony danych w scentralizowanej bazie danych biometrycznych na podstawowe prawa i wolności osób, których dane dotyczą, wydaje się przeważać nad spodziewaną korzyścią wynikającą z przetwarzania danych. W związku z tym przetwarzanie to nie jest zgodne z zasadami konieczności i proporcjonalności. Na tej podstawie EROD stwierdza, że przetwarzanie przewidziane w czwartym scenariuszu **nie może być zgodne z art. 25 RODO**. **Nie byłoby ono również zgodne z art. 5 ust. 1 lit. e) RODO** w oparciu o informacje, którymi dysponuje EROD, oraz **nie byłoby zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO**, gdyby administrator ograniczył się do środków opisanych w tym scenariuszu.

Spis treści

Europejska Rada Ochrony Danych

uwzględniając art. 63 i art. 64 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „**RODO**"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 10 i 22 regulaminu wewnętrznego Europejskiej Rady Ochrony Danych (dalej „**EROD**") (dalej „**regulamin EROD**"),

a także mając na uwadze, co następuje:

(1) Główną rolą EROD jest zapewnienie spójnego stosowania RODO w całym Europejskim Obszarze Gospodarczym (dalej „**EOG**"). Art. 64 ust. 2 RODO stanowi, że każdy organ nadzorczy, przewodnicząca/przewodniczący EROD lub Komisja Europejska mogą wystąpić o przeanalizowanie przez EROD w celu wydania opinii sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim EOG.

(2) EROD przyjmuje opinię zgodnie z art. 64 ust. 3 RODO w związku z art. 10 ust. 2 regulaminu EROD w terminie ośmiu tygodni od podjęcia przez jej przewodniczącą i właściwy organ nadzorczy decyzji o kompletności dokumentacji. Ze względu na złożony charakter sprawy termin ten można przedłużyć o sześć tygodni na podstawie decyzji przewodniczącej.

przyjmuje niniejszą opinię:

1 WPROWADZENIE

1.1 Streszczenie faktów

1. 16 lutego 2024 r. francuski organ nadzorczy zwrócił się do EROD z wnioskiem o wydanie opinii na temat zgodności z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO wykorzystywania technologii rozpoznawania twarzy przez operatorów portów lotniczych i przedsiębiorstwa lotnicze do uwierzytelniania lub identyfikacji pasażerów[2] za pomocą danych biometrycznych w celu usprawnienia przepływu pasażerów w punktach kontroli bezpieczeństwa w porcie lotniczym[3], przy nadawaniu bagażu, podczas wchodzenia na pokład oraz przy wejściu do poczekalni dla pasażerów (z wyłączeniem

[1] Odniesienia do „**państw członkowskich**" zawarte w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG". Odniesienia do „Unii" lub „UE" zawarte w niniejszej opinii należy rozumieć jako odniesienia do „EOG".

[2] W kontekście niniejszej opinii „**pasażer**" oznacza osobę, której dane dotyczą, i której dane osobowe są przetwarzane w konkretnym celu opisanym w niniejszej opinii. W dalszej części opinii pojęcia „pasażer" i „osoba fizyczna" są używane zamiennie.

[3] Do celów niniejszej opinii „**punkty kontroli bezpieczeństwa w porcie lotniczym**" odnoszą się do kontroli bezpieczeństwa przeprowadzanych na odpowiedzialność operatora portu lotniczego, które to kontrole pasażerowie muszą przejść, aby dostać się z hali odlotów do strefy wejścia na pokład lub do punktu przyjęć pasażerów na pokład.

kontroli granicznej i kontroli przeprowadzanych przez sklepy wolnocłowe) (dalej „**wniosek**"). Francuski organ nadzorczy załączył do swojego wniosku opis typowych przypadków użycia (załącznik I).

2. W swoim wniosku francuski organ nadzorczy zauważa, że modele, które są obecnie testowane w kilku portach lotniczych UE, różnią się w poszczególnych państwach członkowskich, co może stwarzać ryzyko rozbieżności interpretacji przez różne organy nadzorcze oraz ryzyko, że w UE wystąpią różne skutki dla podstawowych praw i wolności osób, których dane dotyczą[4].

3. EROD uważa, że aby udzielić odpowiedzi na wniosek, należy odpowiedzieć na następujące pytania:

4. **Pytanie 1**:

1.1. Czy wykorzystanie technologii rozpoznawania twarzy do uwierzytelniania biometrycznego **w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych** (punkty kontroli bezpieczeństwa, nadawanie bagażu, wchodzenie na pokład i wejście do poczekalni dla pasażerów), może być zgodne z **art. 5 ust. 1 lit. f), art. 25 i 32 RODO** w przypadku architektury przechowywania danych, w ramach której wzorzec biometryczny każdego pasażera jest przechowywany **wyłącznie przez osobę fizyczną**, np. lokalnie na jej urządzeniu osobistym, pod jej wyłączną kontrolą?

1.2. Jeżeli takie przetwarzanie zostałoby uznane za zgodne z wyżej wymienionymi przepisami, jakie minimalne odpowiednie zabezpieczenia byłyby potrzebne w świetle art. 25 i 32 RODO?

Pytanie 2:

2.1. Czy wykorzystanie technologii rozpoznawania twarzy do uwierzytelniania lub identyfikacji za pomocą danych biometrycznych **w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych** (punkty kontroli bezpieczeństwa, nadawanie bagażu, wchodzenie na pokład i wejście do poczekalni dla pasażerów), może być zgodne z **art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO** w przypadku **scentralizowanej** architektury przechowywania danych, w ramach której wzorzec biometryczny każdego pasażera jest przechowywany w centralnej bazie danych:

2.1.1. W centralnej bazie danych w porcie lotniczym, pod kontrolą operatora portu lotniczego, w formie zaszyfrowanej, do której klucz dostępu posiada jedynie osoba fizyczna (np. w swoim telefonie komórkowym), do celów uwierzytelniania?

2.1.2. Jeżeli takie przetwarzanie zostałoby uznane za zgodne, jakie minimalne odpowiednie zabezpieczenia byłyby potrzebne w świetle art. 25 i 32 RODO?

2.2.1. W centralnej bazie danych w porcie lotniczym, pod kontrolą operatora portu lotniczego, w formie zaszyfrowanej, do której klucze dostępu posiada operator portu lotniczego, do celów identyfikacji?

2.2.2. Jeżeli takie przetwarzanie zostałoby uznane za zgodne, jakie minimalne odpowiednie zabezpieczenia byłyby potrzebne w świetle art. 25 i 32 RODO?

[4] Wniosek, s. 1.

2.3.1. W chmurze, pod kontrolą przedsiębiorstwa lotniczego lub jego dostawcy usług (podmiotu przetwarzającego), w formie zaszyfrowanej, do której klucze dostępu posiada przedsiębiorstwo lotnicze lub jego dostawca usług, do celów identyfikacji?

2.3.2. Jeżeli takie przetwarzanie zostałoby uznane za zgodne, jakie minimalne odpowiednie zabezpieczenia byłyby potrzebne w świetle art. 25 i 32 RODO?

5. Po tym, jak 16 lutego 2024 r. francuski organ nadzorczy uznał dokumentację za kompletną, a przewodnicząca EROD uznała ją za kompletną 23 lutego 2024 r., Sekretariat rozesłał dokumentację 23 lutego 2024 r. Zgodnie z art. 64 ust. 3 RODO w związku z art. 10 ust. 2 regulaminu EROD przewodnicząca EROD podjęła decyzję o przedłużeniu domyślnego terminu ośmiu tygodni o kolejne sześć tygodni ze względu na złożony charakter sprawy.

1.2 Dopuszczalność wniosku o wydanie opinii na podstawie art. 64 ust. 2 RODO

6. Art. 64 ust. 2 RODO stanowi w szczególności, że każdy organ nadzorczy może wystąpić o przeanalizowanie przez EROD w celu wydania opinii sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim.

7. EROD uważa, że wniosek skierowany przez francuski organ nadzorczy w sprawie zgodności wykorzystywania technologii rozpoznawania twarzy do uwierzytelniania lub identyfikacji za pomocą danych biometrycznych w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych, dotyczy kwestii „wywoływania skutków w więcej niż jednym państwie członkowskim", ponieważ, jak wyjaśniono we wniosku[5], w portach lotniczych państw członkowskich realizowanych jest obecnie kilka projektów i szacuje się, że takie wykorzystywanie wspomnianej technologii wzrośnie w nadchodzących latach. Modele, które są obecnie testowane przez różne porty lotnicze i linie lotnicze, znacznie się różnią w poszczególnych państwach członkowskich, co może stwarzać ryzyko, że z punktu widzenia ochrony danych w więcej niż jednym państwie członkowskim wystąpią rozbieżne skutki.

8. Ponadto EROD uważa, że wniosek złożony przez francuski organ nadzorczy ma istotne konsekwencje dla stosowania zasad określonych w art. 5 ust. 1 lit. e) i f) RODO oraz wymogów mających zastosowanie do administratorów na podstawie art. 25 RODO, a także wymogów mających zastosowanie do administratorów i podmiotów przetwarzających na podstawie art. 32 RODO. W związku z tym wniosek ten dotyczy „sprawy mającej charakter ogólny" w rozumieniu art. 64 ust. 2 RODO, ponieważ odnosi się on do spójnej wykładni zasad ograniczenia przechowywania (art. 5 ust. 1 lit. e) RODO) oraz integralności i poufności (art. 5 ust. 1 lit. f) RODO), a także pojęć ochrony danych w fazie projektowania i domyślnej ochrony danych (art. 25 RODO) oraz bezpieczeństwa danych (art. 32 RODO), aby zapewnić między innymi spójne stosowanie tych przepisów w EOG.

9. Wszelkie ewentualne rozbieżne stanowiska państw członkowskich w sprawie wykładni art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO zwiększyłyby ryzyko, że operatorzy portów lotniczych i przedsiębiorstwa lotnicze będą opracowywać projekty rozpoznawania twarzy w sposób niespójny. Ponieważ francuski organ nadzorczy wykazał wyraźną potrzebę spójnej interpretacji tych przepisów w odniesieniu do technologii rozpoznawania twarzy na potrzeby uwierzytelniania lub identyfikacji pasażerów za

[5] Wniosek, s. 3.

pomocą danych biometrycznych w celu usprawnienia przepływu pasażerów w portach lotniczych[6], EROD uważa, że wniosek jest uzasadniony zgodnie z art. 10 ust. 3 regulaminu EROD.

10. Zgodnie z art. 64 ust. 3 RODO EROD nie wydaje opinii, jeżeli wydała już opinię w danej sprawie[7]. EROD nie udzielała jeszcze odpowiedzi na pytania wynikające z wniosku. Chociaż wytyczne EROD 3/2019 dotyczące urządzeń wideo[8] zawierają już pewne przydatne elementy dotyczące środków bezpieczeństwa, które należy stosować do przetwarzania danych biometrycznych, nie odnoszą się one do wszystkich aspektów dotyczących kwestii poruszonych we wniosku. Ponadto dostępne wytyczne EROD, w tym wytyczne EROD 3/2019 dotyczące urządzeń wideo, nie zawierają szczegółowych wytycznych dotyczących możliwych elementów, które należy zweryfikować w odniesieniu do scentralizowanego lub zdecentralizowanego przechowywania danych biometrycznych do celów identyfikacji lub uwierzytelniania pasażerów w celu usprawnienia przepływu pasażerów w portach lotniczych, ani szczegółowych wytycznych dotyczących zgodności takiego przetwarzania z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO.

11. Z tych powodów EROD uważa, że wniosek jest dopuszczalny, a podniesione w nim kwestie należy przeanalizować w opinii przyjętej na podstawie art. 64 ust. 2 RODO.

2 ZAKRES I KONTEKST OPINII

2.1 Zakres opinii

12. Niniejsza opinia dotyczy wyłącznie tego, czy wykorzystywanie technologii rozpoznawania twarzy do uwierzytelniania lub identyfikacji pasażerów za pomocą danych biometrycznych przez operatorów portów lotniczych i przedsiębiorstwa lotnicze **w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych**, a mianowicie w punktach kontroli bezpieczeństwa, przy nadawaniu bagażu, podczas wchodzenia na pokład i przy wejściu do poczekalni dla pasażerów, jest zgodne z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO.

13. W odniesieniu do **zakresu niniejszej opinii** EROD wyjaśnia, co następuje:

    1) Przetwarzanie danych osobowych w ramach kontroli granicznych i kontroli przeprowadzanych przez sklepy wolnocłowe nie wchodzi w zakres niniejszej opinii, ponieważ jest ono dokonywane przez administratorów innych niż operatorzy portów lotniczych i przedsiębiorstwa lotnicze.

    2) Wykorzystywanie technologii rozpoznawania twarzy, nawet jeśli opiera się na scenariuszach opisanych poniżej w sekcji 3.2, do wszelkich innych celów (takich jak egzekwowanie prawa) lub przez inne strony, nawet w podobnych celach, nie wchodzi w zakres niniejszej opinii.

    3) Opinia dotyczy jedynie przetwarzania danych osobowych pasażerów i nie obejmuje innych rodzajów osób, których dane dotyczą, takich jak pracownicy operatorów portów lotniczych lub przedsiębiorstw lotniczych.

[6] Wniosek, s. 1–3.
[7] Art. 64 ust. 3 RODO i art. 10 ust. 4 regulaminu EROD.
[8] Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo, wersja 2.0, przyjęte 29 stycznia 2020 r. (dalej „**wytyczne EROD 3/2019 dotyczące urządzeń wideo**”).

4) W opinii przeanalizowano wniosek złożony przez francuski organ nadzorczy w odniesieniu do zgodności architektury przechowywania wzorców biometrycznych pasażerów z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO. W tym względzie niniejsza opinia nie zawiera pełnej i całkowitej analizy przestrzegania RODO przez odpowiednich administratorów w każdym przypadku, a także – w stosownych przypadkach – przez ich podmioty przetwarzające. Jest to szczególnie ważne, biorąc pod uwagę, że technologie te pociągają za sobą zwiększone ryzyko związane z przetwarzaniem szczególnych kategorii danych zgodnie z art. 9 RODO. W związku z tym niniejsza opinia pozostaje bez uszczerbku dla oceny dotyczącej innych przepisów RODO w odniesieniu do wykorzystywania technologii rozpoznawania twarzy, w tym w konkretnym sektorze objętym wnioskiem, oraz dla indywidualnej analizy prawnej i technicznej w oparciu o konkretne przewidywane przetwarzanie i okoliczności administratora.

5) Opinia nie dotyczy przetwarzania danych osobowych dzieci i pozostaje bez uszczerbku dla jakichkolwiek szczególnych wymogów mających zastosowanie w tym zakresie.

6) Opinia pozostaje bez uszczerbku dla wymogów prawnych i dalszych ograniczeń dotyczących wykorzystywania danych biometrycznych wynikających z przepisów krajowych państw członkowskich[9].

7) Wszelkie wnioski zawarte w niniejszej opinii pozostają bez uszczerbku dla dalszego rozwoju technologicznego.

8) W opinii przeanalizowano cztery scenariusze, których szczególne cechy opisano poniżej w sekcji 3.2. W opinii nie uwzględniono innych scenariuszy, nawet jeżeli przetwarzanie odbywa się w tych samych celach.

14. W swoim wniosku francuski organ nadzorczy wskazał, że przetwarzanie danych biometrycznych pasażerów w celu usprawnienia przepływu pasażerów w portach lotniczych opierałoby się na założeniu, że osoby fizyczne wyrażają zgodę na takie przetwarzanie, co mogłoby stanowić podstawę prawną na mocy RODO[10]. **Analiza mającej zastosowanie podstawy prawnej nie wchodzi jednak w zakres pytań przedłożonych EROD we wniosku, a zatem ważność zgody na takie przetwarzanie zgodnie z art. 6, 7 i 9 RODO nie jest w niniejszej opinii analizowana.**

15. EROD zauważa jednak ogólnie, że gdyby administratorzy opierali się na tej podstawie prawnej, musieliby uzyskać ważną i wyraźną zgodę[11] od osób, które chcą korzystać z takich usług. Taka wyraźna

[9] Na przykład art. 9 ust. 4 RODO stanowi, że państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych biometrycznych.
[10] Wniosek, załącznik I.
[11] Zgodnie z art. 4 pkt 14 i art. 9 ust. 1 RODO oraz art. 9 ust. 2 lit. a) RODO przetwarzanie danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej jest zakazane, chyba że osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub państwa członkowskiego przewiduje, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w art. 9 ust. 1 RODO. Zob. również motywy 51, 52 i 53 RODO.

zgoda musiałaby być dobrowolna, konkretna i świadoma[12], a kwestia tego, czy warunki te są spełnione, byłaby analizowana indywidualnie dla każdego przypadku. Oznacza to między innymi, że:

1) Osoby fizyczne musiałyby mieć możliwość łatwego wycofania takiej zgody w dowolnym momencie i bez żadnych niekorzystnych konsekwencji[13].

2) Aby udzielenie zgody było dobrowolne, takie wykorzystywanie technologii biometrycznych może odbywać się wyłącznie na zasadzie dobrowolności, ponieważ osoby fizyczne powinny mieć możliwość swobodnego wyboru, czy skorzystać z tych usług, czy też nie, bez żadnych niekorzystnych konsekwencji (takich jak znacznie dłuższe opóźnienia dla pasażerów, którzy nie wyrażą zgody[14]), zachęt, dodatkowych kosztów lub dodatkowych korzyści w zamian[15].

3) Konieczne byłoby również uzyskanie wyraźnej zgody od osób, których dane biometryczne są przetwarzane, nawet jeżeli osoby te nie zostały zarejestrowane w celu ich identyfikacji lub uwierzytelnienia za pomocą takich środków. Innymi słowy, istotne jest, aby kamery nie skanowały twarzy osób, które nie wyraziły wyraźnej zgody na rozpoznawanie twarzy odpowiednio do zamierzonego celu. Można to osiągnąć na przykład poprzez przeznaczenie określonych przejść na potrzeby rozpoznawania twarzy oraz zapewnienie odpowiedniego oznakowania i fizycznego oddzielenia od przepływów pasażerów kontrolowanych w sposób niebiometryczny, aby umożliwić jasną identyfikację takich przejść.

4) Bez uszczerbku dla tego, czy zgoda byłaby mającą zastosowanie podstawą prawną takiego przetwarzania, zasady przetwarzania ustanowione w art. 5 RODO w odniesieniu do konieczności i proporcjonalności nadal mają zastosowanie, nawet jeżeli osoby fizyczne wyraziły wyraźną zgodę na wykorzystywanie ich danych biometrycznych[16].

16. We wniosku określono[17], że operatorzy portów lotniczych pełniliby funkcję administratorów w odniesieniu do przetwarzania danych w punktach kontroli bezpieczeństwa w porcie lotniczym, natomiast przedsiębiorstwa lotnicze pełniłyby funkcję administratorów w odniesieniu do przetwarzania danych przy nadawaniu bagażu, podczas wchodzenia na pokład i przy wejściu do poczekalni dla pasażerów. W związku z tym EROD zauważa, że w przetwarzanie opisane we wniosku mogą być zaangażowane różne podmioty i że nie oceniła zastosowania roli (współ)administratora i podmiotu przetwarzającego w scenariuszach opisanych poniżej w sekcji 3.2 niniejszej opinii. W

[12] Art. 4 pkt 11 i art. 7 RODO.
[13] Art. 7 ust. 4 RODO, a także motyw 50 RODO.
[14] Może to obejmować na przykład kwestie takie jak opracowanie systemu mającego na celu uniknięcie wywierania presji społecznej na pasażerów, którzy nie chcą wyrazić zgody, poprzez uniknięcie sytuacji, w której ich wybór miałby negatywny wpływ na innych pasażerów.
[15] Wytyczne EROD 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, wersja 1.1, przyjęte 4 maja 2020 r. (dalej „**wytyczne EROD 5/2020 dotyczące zgody**"), pkt 46, 48.
[16] Tamże, pkt 5.
[17] Wniosek, załącznik I.

każdym przypadku należy zidentyfikować zaangażowane podmioty i jasno określić ich obowiązki, tak aby spełnione zostały wymogi RODO[18].

17. Ponadto EROD zauważa, że obecnie w UE nie ma jednolitego wymogu prawnego, zgodnie z którym operatorzy portów lotniczych i przedsiębiorstwa lotnicze muszą identyfikować pasażerów i sprawdzać we wszystkich wyżej wymienionych punktach kontroli, czy imię i nazwisko podane na karcie pokładowej pasażera są zgodne z imieniem i nazwiskiem widniejącymi w jego dokumencie tożsamości[19]. W związku z tym wszelkie takie wymogi podlegają przepisom krajowym, które mogą się różnić w poszczególnych państwach członkowskich. W niektórych państwach członkowskich taka weryfikacja może być wymagana w przypadku niektórych punktów kontroli (np. przy nadawaniu bagażu lub wchodzeniu na pokład), podczas gdy w innych państwach członkowskich takie kontrole nie są obecnie wymagane[20]. Istnienie obowiązków prawnych w zakresie weryfikacji tożsamości pasażerów ma bezpośredni wpływ na praktyki poszczególnych portów lotniczych.

18. W związku z tym w takich sytuacjach, **w których weryfikacja tożsamości pasażerów za pomocą urzędowego dokumentu tożsamości nie jest wymagana, nie należy przeprowadzać weryfikacji z wykorzystaniem danych biometrycznych, ponieważ prowadziłoby to do nadmiernego przetwarzania danych, gdyż wiąże się to z przetwarzaniem dodatkowych danych w porównaniu z obecną sytuacją, i wykraczałoby poza to, co jest niezbędne do osiągnięcia odpowiedniego celu, z naruszeniem zasady minimalizacji danych określonej w art. 5 ust. 1 lit. c) RODO**. Należy mieć to na uwadze przy badaniu wszystkich scenariuszy opisanych poniżej w pkt 3.2 niniejszej opinii.

2.2 Główne pojęcia

19. Aby dane zostały zakwalifikowane jako dane biometryczne na podstawie art. 4 pkt 14 RODO[21], przetwarzanie surowych danych, takich jak cechy fizyczne, fizjologiczne lub behawioralne osoby fizycznej, powinno wiązać się z pomiarem tych cech, ponieważ dane biometryczne są wynikiem takich pomiarów[22].

20. Wykorzystując obraz twarzy danej osoby (zdjęcie lub wideo) zwany „**próbką**" biometryczną, możliwe jest wyodrębnienie cyfrowej reprezentacji wyraźnych cech tej twarzy (nazywa się to „**wzorcem**")[23].

---

[18] Zgodnie z art. 4 pkt 7 i 8, art. 5 ust. 2, art. 24, 26, 28 i 29 RODO. Zob. również wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wersja 2.1, przyjęte 7 lipca 2021 r.

[19] Właściwą regulacją na szczeblu UE jest rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego. Rozporządzenie to nie dotyczy jednak kontroli urzędowych dokumentów tożsamości w punktach kontroli w portach lotniczych, a państwa członkowskie mają swobodę regulowania tej kwestii na szczeblu krajowym.

[20] Oznacza to, że obecnie nie przeprowadza się żadnej weryfikacji albo sprawdza się jedynie istnienie karty pokładowej. Na przykład na podstawie protokołu z dnia 22 maja 1954 r. dotyczącego zwolnienia obywateli Danii, Finlandii, Norwegii i Szwecji z obowiązku posiadania paszportu lub dokumentu pobytowego podczas pobytu w państwie skandynawskim innym niż ich własne od dnia 1 lipca 1954 r. obywatele Norwegii, Danii, Finlandii i Szwecji są zwolnieni z obowiązku posiadania paszportu lub innego dowodu tożsamości podczas podróży między tymi państwami.

[21] Zob. również motywy 51, 52 i 53 RODO.

[22] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 74.

[23] Wytyczne EROD 05/2022 w sprawie wykorzystania technologii rozpoznawania twarzy w obszarze ścigania przestępstw, wersja 2.0, przyjęte 26 kwietnia 2023 r. (dalej „**wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw**"), pkt 7 i 8.

Ponadto EROD przypomina, że „[w]zorzec biometryczny jest cyfrową reprezentacją unikalnych cech, które zostały wyodrębnione z próbki biometrycznej i mogą być przechowywane w bazie danych biometrycznych”[24], które to cechy umożliwiają lub potwierdzają jednoznaczną identyfikację osoby fizycznej. Ponadto „[w]zorzec ten ma być unikalny i specyficzny dla każdej osoby i z zasady nie zmienia się z upływem czasu”[25]. Zazwyczaj w procesie porównawczym mającym na celu identyfikację lub uwierzytelnienie osoby za pomocą rozpoznawania twarzy porównuje się wpływający wzorzec biometryczny z identyfikatorami przechowywanymi w celu zweryfikowania dopasowania lub w celu wyszukania go w bazie danych[26].

21. Technologia rozpoznawania twarzy może pełnić dwie odrębne funkcje – uwierzytelniania[27] i identyfikacji[28]. Chociaż obie funkcje są odrębne, obie dotyczą przetwarzania danych biometrycznych związanych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną[29], a zatem stanowią przetwarzanie szczególnych kategorii danych osobowych zgodnie z art. 9 RODO[30].

22. W szczególności:

> **Uwierzytelnianie** ma na celu potwierdzenie przez porównanie, że dana osoba jest tym, za kogo się podaje. Nazywa się to również weryfikacją jeden do jednego.
>
> **Identyfikacja** ma na celu przeszukiwanie bazy danych z zarejestrowanymi danymi biometrycznymi w celu wyszukania identyfikatorów przypisanych do jednej osoby. Nazywa się to również identyfikacją jeden do wielu.

23. W obu przypadkach (tj. identyfikacji i uwierzytelniania) techniki rozpoznawania twarzy opierają się na szacunkowym dopasowaniu między wzorcami; tj. wzorcem porównywanym a bazowym. Z tego punktu widzenia są one oparte na prawdopodobieństwie: porównanie określa wyższe lub niższe prawdopodobieństwo, że dana osoba jest rzeczywiście osobą, która ma zostać uwierzytelniona lub zidentyfikowana; jeśli prawdopodobieństwo to przekroczy określony próg w systemie, zdefiniowany

[24] Tamże, pkt 9.
[25] Tamże.
[26] Wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 10–11; zob. również norma międzynarodowa ISO/IEC 2382-37, 2022-03,
dostępna pod adresem: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [ostatni dostęp w dniu 23 maja 2024 r.] (dalej „**ISO/IEC 2382-37**”)
[27] EROD zauważa, że w przyszłym rozporządzeniu Parlamentu Europejskiego i Rady w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt w sprawie sztucznej inteligencji) (dotychczas nieopublikowanym w Dzienniku Urzędowym) zdefiniowano również w art. 3 pkt 36 „weryfikację biometryczną” jako „zautomatyzowaną weryfikację typu jeden-do-jednego, w tym uwierzytelnianie, tożsamości osób fizycznych przez porównanie ich danych biometrycznych z wcześniej przekazanymi danymi biometrycznymi” (zob. rezolucja ustawodawcza Parlamentu Europejskiego z dnia 13 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
[28] Tamże, w art. 3 pkt 35 aktu w sprawie sztucznej inteligencji zdefiniowano „identyfikację biometryczną” jako „zautomatyzowane rozpoznawanie fizycznych, fizjologicznych, behawioralnych lub psychologicznych cech ludzkich w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z danymi biometrycznymi osób fizycznych przechowywanymi w bazie danych”.
[29] ISO/IEC 2382-37.
[30] Art. 4 pkt 14 RODO i wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 12.

przez użytkownika lub twórcę systemu, system przyjmie, że istnieje zgodność, która ma zostać zidentyfikowana lub uwierzytelniona[31].

[31] Wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 11. Zob. również ISO/IEC 2382-37.

3 W PRZEDMIOCIE ZASADNOŚCI WNIOSKU

3.1 Uwagi ogólne

24. W tej sekcji przeanalizowano pytania przedstawione w pkt 4 powyżej. W tym kontekście EROD przeanalizuje, w odniesieniu do pytania pierwszego, zgodność z art. 5 ust. 1 lit. f) oraz art. 25 i 32 RODO, a w odniesieniu do pytania drugiego – zgodność z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO.

25. W tym celu EROD przeanalizuje cztery różne scenariusze[32], których szczególne cechy opisano poniżej w sekcji 3.2.

26. Na wstępie EROD przypomina, że wykorzystywanie danych biometrycznych, a w szczególności technologii rozpoznawania twarzy, pociąga za sobą zwiększone ryzyko dla praw i wolności osób, których dane dotyczą. Po pierwsze przedmiotowe przetwarzanie dotyczy danych biometrycznych, którym przyznano szczególną ochronę na podstawie art. 9 RODO. W szczególności dane biometryczne bezpowrotnie zmieniają związek między ciałem a tożsamością, ponieważ dzięki nim cechy ludzkiego ciała stają się czytelne dla maszyn i podlegają one dalszemu wykorzystaniu[33]. Ponadto stosowanie technologii rozpoznawania twarzy może prowadzić do ryzyka wystąpienia wyników fałszywie ujemnych, stronniczości i dyskryminacji[34], a możliwość niewłaściwego wykorzystania danych biometrycznych może mieć poważne konsekwencje dla osób, takie jak oszustwa dotyczące tożsamości lub posługiwanie się dokumentem stwierdzającym tożsamość innej osoby[35]. Należy również zauważyć, że w przypadku gdy rozpoznawanie twarzy odbywa się zdalnie i bez aktywnego udziału osoby, której dane dotyczą, osoby mogą być jeszcze mniej świadome takiego przetwarzania i związanego z nim ryzyka. Ponadto należy podkreślić, że cechy, na których opierają się dane biometryczne, można ogólnie uznać za trwałe i należy je traktować jako nieodwołalne, zwłaszcza w kontekście rozpoznawania twarzy[36].

27. W związku z tym, biorąc pod uwagę powyższe, przed zastosowaniem takich technologii, nawet gdyby uznano je za szczególnie skuteczne, administratorzy powinni ocenić wpływ na podstawowe prawa i wolności osób, których dane dotyczą, oraz rozważyć zastosowanie mniej inwazyjnych środków do osiągnięcia prawnie uzasadnionego celu przetwarzania[37].

---

[32] Cztery scenariusze przeanalizowane przez EROD opierają się na przypadkach użycia przedstawionych w załączniku I do wniosku. Francuski organ nadzorczy wyjaśnił, że przypadki użycia przedstawione w załączniku I do wniosku stanowią przykłady wdrożenia należące do scenariusza, wykorzystywane w celach poglądowych.

[33] Opinia 3/2012 Grupy Roboczej Art. 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych przyjęta w dniu 27 kwietnia 2012 r., WP193 (dalej „**opinia 3/2012 Grupy Roboczej Art. 29 w sprawie technologii biometrycznych**"), s. 4. Należy zauważyć, że opinia ta odnosi się do dyrektywy 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych („dyrektywa o ochronie danych"). W RODO rozszerzono zakres szczególnych kategorii danych, a w przeciwieństwie do dyrektywy o ochronie danych RODO stanowi, że dane biometryczne są szczególnymi kategoriami danych (art. 9 RODO).

[34] Wytyczne dotyczące rozpoznawania twarzy, Komitet Doradczy Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, czerwiec 2021 r., s. 15; również wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 27.

[35] Opinia 3/2012 Grupy Roboczej Art. 29 w sprawie technologii biometrycznych, s. 29.

[36] Wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 104.

[37] Motyw 39 RODO. Zob. również wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 73.

28. EROD przypomina również, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym i należy je wyważyć względem innych praw podstawowych chronionych na mocy Karty zgodnie z zasadą proporcjonalności[38].

29. Art. 25 ust. 1 RODO odnosi się do „zasad ochrony danych" wymienionych w art. 5 RODO[39] i wymaga ich „skutecznej realizacji" już w fazie projektowania[40]. Obejmuje to wyraźnie zasadę minimalizacji danych zawartą w art. 5 ust. 1 lit. c) RODO[41], zgodnie z którą dane osobowe muszą być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w jakich są przetwarzane", i która wyraża zasadę proporcjonalności[42]. Ponadto w art. 25 ust. 2 RODO określono obowiązek „domyślnej minimalizacji danych", wskazując przy tym, że obowiązek ten ma zastosowanie do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności[43].

30. Postanowienia art. 25 RODO nie wymagają jednak od administratorów wdrożenia określonych środków technicznych i organizacyjnych, ale wskazują, że wybrane środki i zabezpieczenia powinny odnosić się konkretnie do kontekstu i ryzyka dla praw i wolności osób, których dane dotyczą, wynikającego z przetwarzania[44]. Podobnie art. 32 RODO dotyczący bezpieczeństwa przetwarzania zobowiązuje administratorów i podmioty przetwarzające do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych.

31. Co ważne, nawet gdyby pasażerowie wyraźnie wyrazili zgodę na wykorzystywanie ich danych biometrycznych w celu usprawnienia przepływu pasażerów w portach lotniczych, zasady

---

[38] Motyw 4 RODO. Zob. również w tym względzie wyrok Trybunału Sprawiedliwości z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (dalej „C-439/19 Latvijas Republikas Saeima"), pkt 98, 110 i 113. Ponadto zasada proporcjonalności, jako ogólna zasada prawa Unii, wymaga, by środki wprowadzone aktem Unii były odpowiednie do realizacji zamierzonego celu i nie wykraczały poza to, co jest konieczne do jego osiągnięcia (zob. wyrok Trybunału Sprawiedliwości z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, ECLI:EU:C:2010:662 (dalej „C-92/09 i C-93/09 Volker und Schecke"), pkt 74 i przytoczone tam orzecznictwo).

[39] Wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", wersja 2.0, przyjęte 20 października 2020 r. (dalej „**wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych**"), pkt 11.

[40] Art. 25 ust. 1 RODO stanowi, że: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą". Zob. również wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", pkt 13.

[41] Odpowiednio motyw 39 RODO stanowi, że dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami.

[42] Sprawa C-439/19 Latvijas Republikas Saeima, pkt 98; wyrok Trybunału Sprawiedliwości z dnia 11 grudnia 2019 r., Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (dalej „C-708/18 M5A-ScaraA"), pkt 48.

[43] Wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", pkt 48.

[44] Wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", pkt 14.

przetwarzania zawarte w RODO dotyczące konieczności i proporcjonalności nadal mają zastosowanie i muszą być przestrzegane[45].

32. Jeżeli chodzi o **zasadę konieczności**, EROD przeanalizuje, czy proponowane przetwarzanie jest niezbędne do osiągnięcia zamierzonego celu i czy ten sam cel może zostać zrealizowany w równie skuteczny sposób za pomocą innych środków, w mniejszym stopniu naruszających podstawowe prawa i wolności osób, których dane dotyczą[46]. Jeżeli chodzi o **zasadę proporcjonalności**, EROD oceni, czy negatywny wpływ na podstawowe prawa i wolności osób, których dane dotyczą, jest proporcjonalny do wszystkich przewidywanych korzyści. Jeżeli korzyść jest stosunkowo niewielka, taki wpływ może nie być proporcjonalny[47].

33. W każdym razie, nawet jeżeli EROD uzna, że jeden z analizowanych poniżej scenariuszy może spełniać wymogi określone w art. 5 ust. 1 lit. e) i f), art. 25 i 32 RODO, do administratora należy w każdym przypadku wykazanie tego za pomocą elementów faktycznych. Takie wykazanie powinno obejmować rozważenie alternatywnych scenariuszy.

3.2 W przedmiocie zgodności z art. 5 ust. 1 lit. e) i f), art. 25 i 32 RODO

3.2.1 Scenariusz 1: przechowywanie zarejestrowanego wzorca biometrycznego wyłącznie przez osobę fizyczną do celów uwierzytelniania

34. W tej sekcji przeanalizowano zgodność z art. 5 ust. 1 lit. f) oraz art. 25 i 32 RODO przechowywania wzorca biometrycznego pasażerów wyłącznie przez osobę fizyczną, na przykład na jej urządzeniu osobistym[48], pod jej wyłączną kontrolą[49], do celów uwierzytelniania[50] (dalej „**scenariusz 1**"). W tej sekcji przeanalizowano również odpowiednie zabezpieczenia na potrzeby scenariusza 1 w świetle art. 25 i 32 RODO.

Opis scenariusza

35. W scenariuszu 1 zarejestrowany wzorzec biometryczny każdego pasażera, który wyraził zgodę na takie przetwarzanie, jest przechowywany wyłącznie przez osobę fizyczną, na przykład na urządzeniu osobistym każdego pasażera, pod jego wyłączną kontrolą. Pasażerowie są uwierzytelniani (porównanie 1:1) podczas przechodzenia przez konkretne punkty kontroli w porcie lotniczym.

36. Rejestracji dokonuje operator portu lotniczego albo zdalnie za pośrednictwem aplikacji operatora portu lotniczego[51], albo w terminalach portu lotniczego z odpowiednim poziomem bezpieczeństwa

[45] Wytyczne EROD 5/2020 dotyczące zgody na mocy rozporządzenia 2016/679, pkt 5.
[46] C-439/19 Latvijas Republikas Saeima, pkt 110 i 113; wyrok Trybunału Sprawiedliwości (wielka izba) z dnia 4 lipca 2023 r., Meta przeciwko Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, pkt 108.
[47] C-708/18 M5A-ScaraA, pkt 52–56, C-92/09 i C-93/09 Volker und Schecke, pkt 87, C-439/19 Latvijas Republikas Saeima, pkt 98, 110 i 113. Zob. również opinia 3/2012 Grupy Roboczej Art. 29 w sprawie technologii biometrycznych, s. 9.
[48] Alternatywnie osoba mogłaby wydrukować i przechowywać swój wzorzec biometryczny w formie papierowej.
[49] Pozostaje to bez uszczerbku dla ogólnej odpowiedzialności administratora za przetwarzanie.
[50] Ilustruje to przypadek użycia 1 w załączniku I do wniosku.
[51] EROD zauważa, że w przyszłości można by przewidzieć alternatywne sposoby takiej rejestracji, a rejestrację można by ewentualnie przeprowadzać bez użycia konkretnej aplikacji operatora portu lotniczego, na przykład poprzez interakcję z cyfrowym portfelem użytkownika.

tożsamości (np. z odpowiednim poziomem bezpieczeństwa zgodnie z rozporządzeniem eIDAS[52]). Taka rejestracja polega na zapisaniu na urządzeniu pasażera wzorca biometrycznego i danych identyfikacyjnych[53] (dalej „**dane identyfikacje**") niezbędnych do przetwarzania. Rejestracja jest przeprowadzana tylko raz na określony okres ważności (np. dostosowany do okresu ważności paszportu pasażera). Po zakończeniu procesu rejestracji operator portu lotniczego nie przechowuje ani danych identyfikacyjnych pasażerów, ani ich danych biometrycznych.

37. W szczególności w odniesieniu do przechowywania dane identyfikacyjne i wzorzec biometryczny pasażera są przechowywane lokalnie na urządzeniu każdego pasażera (np. w aplikacji mobilnej operatora portu lotniczego lub w aplikacji cyfrowego portfela). Urządzenie to może zostać następnie wykorzystane do przesłania lub sprawdzenia danych identyfikacyjnych i wzorca biometrycznego pasażera, w tym ewentualnie informacji o locie lub karty pokładowej. Na przykład informacje te są zaszyfrowane kluczem znajdującym się wyłącznie w posiadaniu operatora portu lotniczego – można je zakodować w postaci kodu QR, który można wydrukować na papierze lub wyświetlić na ekranie urządzenia pasażera. W tym przypadku pasażer okazywałby ten kod QR przed dedykowanymi bramkami kontrolnymi w porcie lotniczym, wyposażonymi w skaner QR i kamerę.

38. Jeżeli chodzi o bezpieczeństwo, podczas dopasowywania kody QR zostają odszyfrowane kluczem znajdującym się w posiadaniu operatora portu lotniczego, który jako jedyny może odszyfrować kody QR. Dane biometryczne pasażerów są przechowywane tylko przez bardzo krótki okres i zostają usunięte po zakończeniu dopasowania. Należy zauważyć, że środki bezpieczeństwa w odniesieniu do przechowywania zależą częściowo od bezpieczeństwa urządzenia pasażera.

Ocena przeprowadzona przez EROD

39. W scenariuszu 1 opisano środki techniczne i organizacyjne, które mają zapewnić stopień bezpieczeństwa odpowiadający ryzyku dla osób, których dane dotyczą, zgodnie z wymogami zawartymi w art. 5 ust. 1 lit. f) i art. 32 RODO. Pasażerowie są uwierzytelniani (porównanie 1:1) podczas przechodzenia przez konkretne punkty kontroli w porcie lotniczym. W tym scenariuszu główna operacja dopasowania odbywa się w kontekście kontrolowanego środowiska[54], w którym pasażerowie są aktywnie zaangażowani i mają większą kontrolę nad swoimi danymi. W szczególności jedynie pasażerowie, którzy wyrazili zgodę na takie przetwarzanie, byliby poddawani kontroli, a ponieważ byliby sprawdzani przy dedykowanych bramkach, dane biometryczne innych pasażerów, którzy nie wyrazili zgody na takie przetwarzanie, nie byłyby gromadzone. Ponadto pasażerowie, którzy wyrazili zgodę, mają możliwość wstrzymania przetwarzania danych w dowolnym momencie poprzez usunięcie danych ze swojego urządzenia.

[52] Ramy identyfikacji elektronicznej i usług zaufania (dalej „**eIDAS**") oparte na rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej.

[53] Do celów niniejszej opinii dane identyfikacyjne oznaczają dane, takie jak nazwisko, imię, data urodzenia itp., które zostały zweryfikowane jako dokładne na podstawie dokumentu tożsamości lub paszportu.

[54] „Niekontrolowane środowisko" odnosi się do wykorzystywania rozpoznawania twarzy do celów identyfikacji bez aktywnego zaangażowania osób, których dane dotyczą, gdzie wzorzec każdej twarzy wchodzącej do obszaru monitorowania jest porównywany z wzorcami z szerokiego przekroju populacji przechowywanymi w bazie danych, zob. wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 17.

40. Rozpoznawanie twarzy w oparciu o wzorzec biometryczny przechowywany wyłącznie przez osobę fizyczną, na przykład na urządzeniu osobistym pasażera pod jego wyłączną kontrolą, wykorzystywane do uwierzytelniania w konkretnych punktach kontroli za pośrednictwem dedykowanego interfejsu, stwarza – w pewnych warunkach – mniejsze ryzyko w porównaniu z wykorzystaniem danych biometrycznych, w przypadku gdy dane te są przechowywane w scentralizowanej bazie danych[55]. Takie lokalne przechowywanie, o ile towarzyszą mu odpowiednie zabezpieczenia[56], zmniejsza dotkliwość naruszeń ochrony danych osobowych w porównaniu ze scentralizowanym przechowywaniem, jeżeli chodzi o liczbę poszkodowanych osób, oraz zapewnia, aby dostęp do wzorca biometrycznego obejmował aktywne zaangażowanie osoby, której dane dotyczą.

41. Ponadto dopasowanie można przeprowadzić lokalnie w porcie lotniczym poprzez porównanie wzorca biometrycznego, na przykład zawartego w kodzie QR, z wynikiem uzyskanym z wzorca, obliczonym na podstawie próbki biometrycznej uchwyconej przez kamerę bramki kontrolnej. Jedynie pozytywny wynik dopasowania zostałby podany do wiadomości kontrolerowi przeprowadzającemu konkretną kontrolę i wykorzystany przez niego (może to być operator portu lotniczego lub przedsiębiorstwo lotnicze, w zależności od tego, czy kontrola odbywa się w punktach kontroli bezpieczeństwa w porcie lotniczym, przy nadawaniu bagażu, podczas wchodzenia na pokład czy przy wejściu do poczekalni dla pasażerów). Ponadto fakt, że informacje wymagane do dopasowania (np. kod QR) muszą być podane przez osobę fizyczną, stanowi drugi czynnik[57], co tym samym wzmacnia bezpieczeństwo uwierzytelniania.

42. Jeżeli chodzi o zgodność z art. 25 RODO, w szczególności w celu spełnienia wymogu minimalizacji danych, należy zapewnić, aby przetwarzanie było zgodne z zasadą konieczności. W scenariuszu 1 można uznać, że wybrane środki są zgodne z zasadą konieczności w odniesieniu do zamierzonego celu (tj. usprawnienia przepływu pasażerów), jeżeli – w zależności od okoliczności przetwarzania – administrator jest w stanie wykazać, że nie istnieją mniej inwazyjne rozwiązania alternatywne, które mogłyby przyczynić się do równie skutecznego osiągnięcia tego samego celu. Na przykład administrator może być w stanie wykazać, że nawet jeśli pasażerowie musieliby pokazać swoje urządzenie, scenariusz 1 przyspiesza proces weryfikacji w porównaniu z obecną sytuacją, która obejmuje sprawdzenie przez człowieka, czy imię i nazwisko podane na karcie pokładowej są zgodne z imieniem i nazwiskiem widniejącymi w dokumencie tożsamości pasażera[58]. W szczególności nie można tego wykazać, jeżeli obecnie nie przeprowadza się kontroli tożsamości pasażerów na podstawie ich oficjalnego dokumentu tożsamości (zob. w tym względzie pkt 18 powyżej).

43. Ponadto operatorzy portu lotniczego nie przechowują wzorców biometrycznych po ich zarejestrowaniu, a okres przechowywania danych biometrycznych przez kontrolera przeprowadzającego kontrolę jest bardzo krótki, ponieważ takie dane są usuwane natychmiast po przeprowadzeniu dopasowania. W związku z tym środki wybrane w scenariuszu 1 wydają się ograniczać zakres przetwarzania i okres przechowywania danych osobowych.

---

[55] Wytyczne EROD 5/2022 w sprawie rozpoznawania twarzy w obszarze ścigania przestępstw, pkt 17.

[56] Omówione poniżej w pkt 46.

[57] Na przykład ogranicza to ryzyko spoofingu tożsamości. Zob. również zabezpieczenie omówione w sekcji C.1.2 poniżej.

[58] Można również przyjąć, że kontrola biometryczna może być mniej podatna na błędy w porównaniu z kontrolą przeprowadzaną przez człowieka.

44. Jeżeli chodzi o zasadę proporcjonalności, inwazyjność takiego przetwarzania można zrównoważyć aktywnym zaangażowaniem pasażerów, ponieważ ich dane biometryczne byłyby przechowywane wyłącznie przez nich. Ponadto, biorąc pod uwagę środki opisane powyżej i zakładając, że administrator wdroży odpowiednie zabezpieczenia wymagane w przypadku tego konkretnego przetwarzania, wdrożenie odpowiednich środków mogłoby zapewnić stopień bezpieczeństwa odpowiadający ryzyku. W takim przypadku negatywny wpływ na podstawowe prawa i wolności osób, których dane dotyczą, można uznać za proporcjonalny do spodziewanych korzyści.

45. W związku z powyższym w odpowiedzi na pytanie 1.1 EROD stwierdza, że takie przetwarzanie **można uznać za zasadniczo zgodne z art. 5 ust. 1 lit. f) oraz art. 25 i 32 RODO, z zastrzeżeniem odpowiednich zabezpieczeń**.

Odpowiednie zabezpieczenia

46. W tego rodzaju scenariuszu, w odpowiedzi na pytanie 1.2, EROD uważa, że należy wdrożyć co najmniej poniżej opisane zabezpieczenia. Zabezpieczenia inne niż te opisane w niniejszej opinii można wykorzystać do osiągnięcia tych samych celów w zakresie bezpieczeństwa i ochrony danych i mogą one być zgodne z prawem, o ile zapewniają zgodność z mającymi zastosowanie ramami prawnymi.

47. Uwaga: jest to ogólny i niewyczerpujący przegląd możliwych odpowiednich zabezpieczeń, które administrator powinien wdrożyć w rozwiązaniu podobnym do scenariusza 1. Odpowiedniość zabezpieczeń na podstawie art. 25 i 32 RODO będzie zależała od analizy poszczególnych przypadków. Wszyscy administratorzy będą musieli zapewnić przeprowadzenie własnej oceny skutków dla ochrony danych[59], a ich konkretne rozwiązania mogą wymagać dodatkowych środków nieuwzględnionych w niniejszej opinii.

A. Kwestie ogólne

A.1 Ocena skutków przetwarzania danych

A.1.1 Należy przeprowadzić ocenę skutków dla ochrony danych, zgodnie z wymogami art. 35 RODO, za każdym razem, gdy administrator planuje nową operację przetwarzania obejmującą przetwarzanie, które może wiązać się z wysokim ryzykiem. Dotyczy to prawdopodobnie scenariusza 1, ponieważ wiąże się on z przetwarzaniem danych biometrycznych na dużą skalę[60]. Należy ocenić adekwatność wdrożenia systemu rozpoznawania twarzy, w tym jego niezbędność i proporcjonalność w stosunku do zamierzonych celów[61], na wczesnym etapie projektowania i dokonywać jego przeglądu w całym cyklu życia produktu.

[59] Art. 35 RODO.
[60] Art. 35 ust. 3 RODO i wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, przyjęte 13 października 2017 r., WP248rev.01, zatwierdzone przez EROD.
[61] Art. 35 ust. 7 lit. b) RODO.

A.1.2 Należy skonsultować się z właściwym organem nadzorczym, jeżeli przetwarzanie nadal powoduje wysokie ryzyko pomimo zastosowania przez administratora środków w celu zminimalizowania tego ryzyka[62].

A.2 Prawa osób, których dane dotyczą, i zabezpieczenia, które mogą wdrożyć administratorzy danych

A.2.1 Należy wdrożyć zabezpieczenia mające na celu przeciwdziałanie wystąpieniu wyników fałszywie ujemnych. Należy ograniczyć ryzyko nierównego traktowania ze względu na wiek, płeć i rasę, przeprowadzając systematyczną ocenę funkcjonowania algorytmów zgodnie z celami i dostosowując algorytmy, aby ograniczyć wykryte problemy dotyczące nierównego traktowania i zapewnić rzetelność w procesie przetwarzania[63]. Na przykład poprzez wdrożenie nadzoru ludzkiego i interwencji ludzkiej w celu ograniczenia ryzyka nierównego traktowania i zapewnienia, aby nie dochodziło do stygmatyzacji ani profilowania pasażerów.

A.2.2 Należy zapewnić, aby wszelkie przetwarzanie danych osobowych było przejrzyste, a osoby fizyczne miały świadomość tego oraz kontrolę nad tym, w jaki sposób ich dane są przetwarzane, w odniesieniu do każdej operacji przetwarzania[64].

A.2.3 Należy zapewnić środki zapewniające zgodność z zasadą ograniczenia celu, tak aby dane nie były wykorzystywane do innych celów, takich jak cele w zakresie bezpieczeństwa lub szkoleń.

A.2.4 Należy zapewnić, aby żadne zdjęcia lub wideo, nawet jeżeli nie będą zapisywane i przetwarzane, nie były rejestrowane od osób, które nie wyraziły zgody na rozpoznawanie twarzy, za pomocą odpowiednich środków (takich jak stosowanie odpowiedniej głębokości pola i odpowiedniego obszaru uchwycenia w celu uniknięcia rejestrowania obrazów od innych pasażerów znajdujących się w tle lub obok, wykorzystywanie dedykowanych kolejek wyraźnie oznaczonych jako kolejki do celów rozpoznawania twarzy).

A.2.5 W przypadku gdy te same czytniki mogą być używane przez pasażerów wyrażających zgodę na rozpoznawanie twarzy i niewyrażających zgody na rozpoznawanie twarzy lub jeżeli pasażerowie, którzy nie wyrażają zgody na rozpoznawanie twarzy, mogą pojawić się w polu widzenia w czasie, gdy system nie jest używany, należy poczekać na pozytywne działanie pasażera, który wyraził zgodę, zanim rozpocznie się rejestrowanie zdjęcia lub wideo.

[62] Art. 36 ust. 1 RODO.
[63] Wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", przypis 60, pkt 70.
[64] Wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", pkt 68, oraz motyw 7 RODO.

A.2.6 Należy umożliwić osobie, której dane dotyczą, usunięcie w dowolnym momencie danych przechowywanych wyłącznie przez nią (wzorzec biometryczny[65]) w aplikacji mobilnej lub cyfrowym portfelu[66].

A.2.7 Należy zapewnić istnienie realnych rozwiązań alternatywnych lub rozwiązań zapasowych (tj. dla pasażerów, którzy nie wyrazili zgody na wykorzystanie swoich danych biometrycznych, dla pasażerów, którzy nie są w stanie skorzystać z takich rozwiązań, lub dla pasażerów, którzy doświadczyli bezpodstawnych odrzuceń), tak aby zagwarantować również, by pasażerowie, którzy nie wyrazili zgody, nie odczuli żadnych niekorzystnych konsekwencji[67].

A.2.8 W przypadku używania aplikacji należy ją starannie zaprojektować i skonfigurować, aby nie gromadzić zbędnych danych i aby uniknąć wykorzystywania jakichkolwiek zestawów do opracowywania oprogramowania osób trzecich („SDK") gromadzących dane do innych celów.

A.3 Rozliczalność

A.3.1 Należy ocenić, czy istnieją jakiekolwiek odpowiednie kodeksy postępowania lub mechanizmy certyfikacji, które mają pomóc w wykazaniu zgodności z bezpieczeństwem przetwarzania określonym w art. 32 RODO[68]. Należy sprawdzić odpowiedniość środków w odniesieniu do przedmiotowego przetwarzania. Normy[69], najlepsze praktyki i kodeksy postępowania, które są uznawane przez stowarzyszenia i inne organy reprezentujące kategorie administratorów, mogą być przydatne w ustalaniu odpowiednich środków.

A.3.2 Należy zapewnić przeprowadzanie podstawowych kontroli bezpieczeństwa na urządzeniu użytkownika, aby umożliwić fazę rejestracji, mimo że pasażer również odpowiada za ochronę swoich danych, ponieważ są one przechowywane na jego urządzeniu. Przykłady takich weryfikacji i kontroli technicznych przedstawiono poniżej w sekcji C.2 „Infrastruktura i sieć".

B. Kwestie organizacyjne:

B.1 Polityka i zgodność

[65] Odniesienia do wzorca biometrycznego w zabezpieczeniach przewidzianych w scenariuszu 1 odpowiadają odniesieniom do klucza dostępu w scenariuszu 2.
[66] Należy mieć na uwadze, że to zabezpieczenie ma zastosowanie wyłącznie do scenariusza 1.
[67] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 86.
[68] Art. 32 ust. 3 RODO i wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", pkt 10.
[69] Zob. na przykład ISO/IEC 2382-37.

B.1.1 Należy zapewnić wprowadzenie wewnętrznych kontroli dostępu[70] wraz z zasadami dotyczącymi administratorów.

B.1.2 Jeżeli usługa rozpoznawania twarzy może być świadczona przez jedną ze stron zaangażowanych w przetwarzanie danych bez danych identyfikacyjnych, danych biometrycznych lub obu rodzajów danych, które muszą być przetwarzane przez inne zaangażowane strony, należy zakazać przepływu tych danych przez te inne strony. Na przykład przedsiębiorstwo lotnicze nie musi mieć technicznego dostępu do danych biometrycznych, jeżeli korzysta ze wspólnej infrastruktury portu lotniczego, nawet jeżeli to przedsiębiorstwo lotnicze działa jako administrator przetwarzania danych na podstawie RODO.

B.1.3 Należy określić politykę w zakresie szyfrowania i zarządzania kluczami[71], np. w odniesieniu do przetwarzania danych identyfikacyjnych i biometrycznych.

B.1.4 Należy zapewnić zgodność z rozdziałem V RODO. Na przykład należy zapewnić zgodne z przepisami przekazywanie danych, jeżeli administrator korzysta z usługi zdalnej w trakcie procesu rejestracji zlokalizowanego w państwie trzecim.

B.1.5 W przypadku korzystania z usług podmiotów przetwarzających należy zapewnić zawarcie umowy dotyczącej przetwarzania danych[72] zgodnie z art. 28 ust. 3 RODO.

B.1.6 Należy zapewnić wprowadzenie procedur zarządzania nadzorem ludzkim i interwencją ludzką, w szczególności w celu rozwiązywania problemów związanych z bezpodstawnym odrzuceniem oraz problemów technicznych lub związanych z użytecznością.

B.2 Szkolenia i testy

B.2.1 Należy zapewnić odpowiednie przeszkolenie personelu.

B.2.2 Należy wdrożyć „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania”[73].

B.2.3 Należy wdrożyć proces zapewniający, aby przetwarzanie wzorca biometrycznego[74] pasażera do celów uwierzytelniania było skuteczne pod względem technicznym i wystarczająco dokładne.

---

[70] Wytyczne EROD 04/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19, przyjęte 21 kwietnia 2020 r. (dalej „**wytyczne EROD 4/2020 w sprawie danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych**”), BEZP-10, s. 19.

[71] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 89.

[72] Art. 28 ust. 3 RODO.

[73] Art. 32 ust. 1 lit. d) RODO.

[74] Odniesienia do wzorca biometrycznego w zabezpieczeniach przewidzianych w scenariuszu 1 odpowiadają odniesieniom do klucza dostępu w scenariuszu 2.

B.2.4 Należy zapewnić, aby próbki biometryczne pobrane podczas rejestracji oraz w punkcie kontroli miały jakość wystarczającą do przeprowadzenia wiarygodnego przetwarzania danych biometrycznych.

C. Kwestie techniczne:

C.1 Dostęp

C.1.1 Należy wdrożyć zabezpieczenia na etapie rejestracji w celu zapewnienia zastosowania metody bootstrap w stosunku do procesu rejestracji przy użyciu zweryfikowanej tożsamości. Na przykład, aby wzmocnić ocenę uwierzytelniania wieloskładnikowego tożsamości użytkowników, można wdrożyć kroki, począwszy od jednorazowych linków chronionych hasłem służących do uruchomienia aplikacji, po lokalne mechanizmy odblokowania urządzeń.

C.1.2 Należy wdrożyć zabezpieczenia mające na celu przeciwdziałanie wystąpieniu wyników fałszywie dodatnich i atakom prezentacyjnym oraz zapobieganie oszustwom[75].

C.1.3 Należy zakazać jakiegokolwiek dostępu do danych identyfikacyjnych i biometrycznych z zewnątrz[76].

C.1.4 Należy zapewnić, aby przetwarzanie odbywało się lokalnie na etapach rejestracji, przesyłania i dopasowania. Jednostka dopasowująca powinna znajdować się jak najbliżej urządzenia danej osoby. Umożliwienie dopasowania wzorca na urządzeniu osobistym może wymagać interakcji z dostawcami usług znajdującymi się poza portem lotniczym i wykorzystania publicznych zasobów sieciowych, czego wadą byłby wpływ na dostępność wzorca i udostępnianie go podmiotom zewnętrznym.

C.1.5 Należy uwierzytelnić użytkownika, aby dodać nowy lot i wygenerować nowy zaszyfrowany kod QR.

C.1.6 Należy wdrożyć środki mające na celu zaradzenie sytuacji, w której pasażer może stracić dostęp do swojego kodu QR.

C.2 Infrastruktura i sieć

C.2.1 Należy zapewnić aktualizację warunków dotyczących systemu operacyjnego i umożliwić uwierzytelnianie do celów uzyskania dostępu do urządzenia, tak aby zapewnić działanie aplikacji/cyfrowego portfela, w tym z automatycznym usuwaniem danych identyfikacyjnych i biometrycznych, jeżeli system operacyjny jest przestarzały i stwarza zagrożenie dla bezpieczeństwa.

[75] Sprawozdanie ENISA ze stycznia 2022 r. w sprawie tożsamości cyfrowej w odniesieniu do wykorzystywania koncepcji tożsamości suwerennej (SSI) do budowy zaufania.
[76] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 89.

C.2.2 Należy odłączyć jednostki dopasowujące (tj. czytniki) od sieci podczas użycia oraz podjąć wszelkie inne niezbędne środki w celu zapewnienia bezpieczeństwa.

C.2.3 Należy wykonywać dopasowanie danych biometrycznych na urządzeniu pasażera lub na czytniku (przetwarzanie brzegowe).

C.2.4 Należy opracować rozwiązania mające na celu wyeliminowanie luk w zabezpieczeniach urządzeń osobistych pasażerów, w tym szyfrowanie (co najmniej) przechowywanych danych biometrycznych i danych identyfikacyjnych.

C.2.5 Należy stosować bezpieczne przechowywanie (co najmniej) danych biometrycznych posiadanych wyłącznie przez użytkownika[77], na przykład poprzez zastosowanie modułu „bezpiecznej enklawy" na smartfonie.

C.2.6 Należy zastosować zabezpieczenia zapewniające bezpieczeństwo fizyczne obiektów, w tym terminalu biometrycznego portu lotniczego. Należy zapewnić wysoki poziom bezpieczeństwa elementów architektury, które przetwarzają dane identyfikacyjne i biometryczne (np. obliczenia, przepływ danych, przechowywanie krótkotrwałe lub długoterminowe).

C.3 Kontrola tożsamości użytkownika – bezpieczeństwo danych i zarządzanie danymi

C.3.1 Należy zapewnić kategoryzację danych w trakcie ich przesyłania i przechowywania na co najmniej trzy grupy, takie jak: dane identyfikacyjne, dane biometryczne i dane dotyczące lotu[78]. Należy zapewnić odpowiednie szyfrowanie danych między przekazywaniem a przechowywaniem.

C.3.2 Należy wprowadzić środki techniczne w celu zapewnienia, aby w danym punkcie kontroli przetwarzane i weryfikowane były wyłącznie takie dane, które zgodnie z prawem mogą być przetwarzane w takich konkretnych punktach kontroli.

C.3.3 Należy zapewnić skuteczność usuwania danych[79] za pomocą bezpiecznej procedury usuwania (np. pamięć główna, pamięć podręczna, potencjalne kopie zapasowe) oraz ocenić, kiedy usuwanie danych powinno być zautomatyzowane. Okresy przechowywania danych powinny być ściśle przestrzegane za pomocą automatycznych rutynowych procedur, bez konieczności podejmowania dodatkowych działań przez osobę fizyczną[80].

[77] Odniesienia do wzorca biometrycznego w zabezpieczeniach przewidzianych w scenariuszu 1 odpowiadają odniesieniom do klucza dostępu w scenariuszu 2.
[78] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 89.
[79] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 89.
[80] Wytyczne EROD 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych", pkt 82.

C.3.4 Należy zapewnić autentyczność i integralność danych (na przykład za pomocą podpisu)[81].

C.3.5 Należy zachowywać dane biometryczne pasażerów w punkcie rejestracji i w punkcie kontroli tylko przez bardzo krótki okres i usuwać je niezwłocznie po przejściu pasażera przez punkt kontroli.

C.3.6 Jeżeli do rejestracji wykorzystywana jest aplikacja, należy stosować normy bezpieczeństwa dla aplikacji mobilnych podczas opracowywania aplikacji, a także testy bezpieczeństwa przeprowadzane przez stronę trzecią.

C.3.7 Należy zapewnić środki bezpieczeństwa na etapie rejestracji w porcie lotniczym w celu zachowania poufności i integralności danych biometrycznych pasażera. Na przykład, jeżeli kod QR jest drukowany przez kiosk, nie powinien on być wyświetlany w kiosku, aby uniknąć robienia zdjęcia przez podmiot działający w złej wierze. W przypadku transmisji na niewielkich odległościach transmisja powinna być przeprowadzana w oparciu o aktywne zaangażowanie użytkownika i za pośrednictwem kanału zapewniającego bliskość.

C.3.8 Dane posiadane wyłącznie przez osobę fizyczną[82] powinny być przechowywane w bezpiecznym miejscu na urządzeniu osobistym danej osoby, a wszelkie ewentualne podatności związane z systemami operacyjnymi urządzenia muszą zostać poddane odpowiednim poprawkom zabezpieczeń. W przypadku wydrukowanego kodu QR osoba powinna zostać poinformowana o szczególnie wrażliwym charakterze zawartych w nim danych oraz o tym, co można zrobić za pomocą tego kodu.

C.3.9 Należy zapewnić, aby rejestracja była przeprowadzana z wykorzystaniem odpowiednich technik zdalnej weryfikacji tożsamości[83].

3.2.2 Scenariusz 2: scentralizowane przechowywanie zarejestrowanego wzorca biometrycznego w porcie lotniczym w formie zaszyfrowanej, do której klucz dostępu posiada wyłącznie pasażer, do celów uwierzytelniania

48. W tej sekcji przeanalizowano zgodność z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO scentralizowanego przechowywania, do celów uwierzytelniania, zarejestrowanych wzorców biometrycznych pasażerów w centralnej bazie danych w formie zaszyfrowanej, do której klucz dostępu posiada wyłącznie pasażer[84] (dalej „**scenariusz 2**"). W sekcji tej przeanalizowano również odpowiednie zabezpieczenia na potrzeby scenariusza 2 w świetle art. 25 i 32 RODO.

Opis scenariusza

[81] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 89.
[82] Odniesienia do wzorca biometrycznego w zabezpieczeniach przewidzianych w scenariuszu 1 odpowiadają odniesieniom do klucza dostępu w scenariuszu 2.
[83] Zob. sprawozdanie ENISA w sprawie zdalnej weryfikacji tożsamości: analiza metod przeprowadzania zdalnej weryfikacji tożsamości, marzec 2021 r.
[84] Ilustruje to przypadek użycia 2 w załączniku I do wniosku.

49. W scenariuszu 2 rejestracja jest przeprowadzana tylko raz na dany okres ważności (na przykład rok po ostatnim locie, do upływu ważności paszportu) albo zdalnie z odpowiednim poziomem bezpieczeństwa tożsamości (np. z odpowiednim poziomem bezpieczeństwa zgodnie z rozporządzeniem eIDAS), albo w terminalach portu lotniczego. Rejestrację kontroluje operator portu lotniczego i polega ona na wygenerowaniu danych identyfikacyjnych i danych biometrycznych zaszyfrowanych kluczem.

50. Baza danych jest przechowywana na terenie portu lotniczego pod kontrolą operatora portu lotniczego. Osobiste klucze kryptograficzne są przechowywane wyłącznie na urządzeniu danej osoby (np. w aplikacji mobilnej operatora portu lotniczego). Aplikacja może wygenerować kod QR zawierający klucz, który można wydrukować na papierze lub wyświetlić na ekranie urządzenia[85]. Ponadto operator portu lotniczego wykonuje drugą warstwę szyfrowania[86] za pomocą kluczy znajdujących się pod kontrolą operatora portu lotniczego.

51. Pasażerowie są uwierzytelniani (porównanie 1:1) podczas przechodzenia przez konkretne punkty kontroli w porcie lotniczym Pasażerowie, którzy wybrali przejście przez punkty kontroli biometrycznej, okazują swój kod QR przed dedykowaną bramką kontrolną wyposażoną w skaner QR i kamerę. Indeks pasażera jest wysyłany do bazy danych w celu zażądania zaszyfrowanego wzorca, który jest pobierany i sprawdzany lokalnie na czytniku lub urządzeniu użytkownika. Jedynie pozytywny wynik dopasowania jest podawany do wiadomości kontrolera punktu kontroli i wykorzystywany przez niego[87].

52. W tym scenariuszu między portami lotniczymi nie następują przepływy danych identyfikacyjnych i biometrycznych, a scentralizowane bazy danych nie są ze sobą połączone oraz nie współdziałają między sobą.

Ocena przeprowadzona przez EROD

53. W scenariuszu 2 zarejestrowane wzorce biometryczne pasażerów są przechowywane w sposób scentralizowany, ale w formie zaszyfrowanej, do której klucz dostępu posiadają jedynie pasażerowie. W scenariuszu 2 pasażerowie są uwierzytelniani (porównanie 1:1).

54. W tym scenariuszu proponuje się, aby cel polegający na usprawnieniu przepływu pasażerów (tj. poprzez przyspieszenie kontroli) można było osiągnąć za pomocą scentralizowanego systemu. EROD już wcześniej zauważyła, że takie rozwiązanie można uznać za realną alternatywę dla zdecentralizowanego przechowywania zarejestrowanych wzorców biometrycznych[88] (jak opisano w scenariuszu 1), jeżeli istnieją obiektywne potrzeby oraz przy zastosowaniu odpowiednich zabezpieczeń (zob. zabezpieczenia opisane w pkt 60 poniżej).

55. Jeżeli chodzi o kwestie bezpieczeństwa, dane każdej osoby są szyfrowane za pomocą konkretnego klucza przechowywanego wyłącznie przez daną osobę oraz pod jej wyłączną kontrolą. Ponadto fakt,

[85] Francuski organ nadzorczy doprecyzował również inne rozwiązania techniczne umożliwiające przesyłanie wymaganych informacji, takie jak stosowanie protokołu komunikacji na niewielkich odległościach.
[86] Klucz dostępu (znajdujący się w posiadaniu osoby fizycznej) jest sam w sobie zaszyfrowany innym kluczem znajdującym się w posiadaniu operatora portu lotniczego.
[87] Francuski organ nadzorczy wyjaśnił, że ten okres przechowywania ma charakter przykładowy i może zostać uznany za dopuszczalny, biorąc pod uwagę, że klucz znajduje się w posiadaniu osób fizycznych i może zostać wybrany na etapie rejestracji. Należy jednak zauważyć, że taki okres przechowywania może zostać dostosowany.
[88] Wytyczne EROD 3/2019 dotyczące urządzeń wideo, pkt 88.

że informacje wymagane do dopasowania (tj. klucz dostępu) muszą być podane przez osobę fizyczną, stanowi drugi czynnik uwierzytelniania[89], co wzmacnia bezpieczeństwo uwierzytelniania. Ponadto operator portu lotniczego wykonuje drugą warstwę szyfrowania za pomocą kluczy znajdujących się pod kontrolą operatora portu lotniczego. W scenariuszu 2 indeks osoby fizycznej jest przesyłany do centralnej bazy danych w celu pozyskania danych biometrycznych związanych z daną osobą. Dane te są następnie przesyłane (w formie zaszyfrowanej) do komputera zlokalizowanego w punkcie kontroli, w którym zostają odszyfrowane w celu dokonania dopasowania, a jedynie pozytywny wynik dopasowania jest podawany do wiadomości kontrolera w punkcie kontroli i przez niego wykorzystywany. Takie środki bezpieczeństwa można zatem uznać za zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO, pod warunkiem że klucz dostępu osoby fizycznej jest przechowywany w komputerze zlokalizowanym w punkcie kontroli oraz że do centralnej bazy danych zostanie przesłany jedynie indeks pasażera w celu wyszukania zaszyfrowanego wzorca biometrycznego.

56. Jeżeli chodzi o zgodność z art. 25 RODO, w szczególności w celu spełnienia wymogu minimalizacji danych, należy zapewnić, aby przetwarzanie było zgodne z zasadą konieczności. W scenariuszu 2 można uznać, że wybrane środki są zgodne z zasadą konieczności w odniesieniu do zamierzonego celu (tj. usprawnienia przepływu pasażerów w portach lotniczych), jeżeli – w zależności od okoliczności przetwarzania – administrator jest w stanie wykazać, że nie istnieją mniej inwazyjne rozwiązania alternatywne, które mogłyby przyczynić się do równie skutecznego osiągnięcia tego samego celu. W scenariuszu 2 pasażerowie nadal musieliby pokazać swoje urządzenie[90]. Niemniej jednak administrator może być w stanie wykazać, że scenariusz 2 przyspiesza proces weryfikacji w porównaniu z obecną sytuacją, która obejmuje sprawdzenie przez człowieka, czy imię i nazwisko podane na karcie pokładowej są zgodne z imieniem i nazwiskiem widniejącymi w dokumencie tożsamości pasażera[91], lub w porównaniu ze scenariuszem 1. W szczególności nie można tego wykazać, jeżeli obecnie nie przeprowadza się kontroli tożsamości pasażerów na podstawie ich oficjalnego dokumentu tożsamości (zob. w tym względzie pkt 18 powyżej).

57. Jeżeli chodzi o zasadę proporcjonalności, inwazyjność takiego przetwarzania można zrównoważyć aktywnym zaangażowaniem pasażerów, którzy posiadają pod swoją wyłączną kontrolą klucz dostępu do zaszyfrowanych danych. Ponadto wydaje się, że zagrożenia bezpieczeństwa związane z przechowywaniem danych biometrycznych pasażerów w scentralizowanej bazie danych oraz z kluczem dostępu znajdującym się wyłącznie w posiadaniu pasażerów można by ograniczyć za pomocą odpowiednich zabezpieczeń (zob. zabezpieczenia, o których mowa w pkt 60 poniżej). W związku z tym, zakładając, że administrator wdroży odpowiednie zabezpieczenia wymagane w przypadku tego konkretnego przetwarzania, zagrożenia dla osób fizycznych można by ograniczyć, a negatywny wpływ na podstawowe prawa i wolności osób, których dane dotyczą, można uznać za proporcjonalny do spodziewanych korzyści. Oczywiście w każdym przypadku należy zadbać o to, aby przetwarzane były wyłącznie dane potrzebne do danego celu oraz aby jedynie pasażerowie, którzy wyrazili zgodę, byli

[89] Na przykład ogranicza to ryzyko spoofingu tożsamości. Zob. również zabezpieczenie omówione w sekcji C.1.2.
[90] Francuski organ nadzorczy doprecyzował również inne możliwości okazania wzorca, np. wydrukowanego na papierze. Ponadto EROD uznaje, że w przyszłości można by przewidzieć wykorzystanie alternatywnej technologii, np. opartej na systemie komunikacji bliskiego zasięgu.
[91] Można również przyjąć, że kontrola biometryczna może być mniej podatna na błędy w porównaniu z kontrolą przeprowadzaną przez człowieka.

poddawani kontroli, w związku z czym nie istnieje ryzyko, że gromadzone byłyby dane biometryczne innych pasażerów, którzy nie wyrazili zgody.

58. We wniosku podano jako przykład, że w scenariuszu 2 okres przechowywania zaszyfrowanych danych w bazie danych może zwykle wynosić rok po ostatnim locie odbytym przez osobę fizyczną, do upływu ważności paszportu. We wniosku nie przedstawiono żadnych informacji w celu uzasadnienia tak długiego okresu w oparciu o obiektywne powody, chociaż można założyć, że taki okres przechowywania jest przewidziany ze względu na wygodę podczas lotów w przyszłości. Jeżeli chodzi o okres przechowywania danych, aby w tym scenariuszu osiągnąć zgodność z art. 5 ust. 1 lit. e) RODO, administratorzy powinni być w stanie uzasadnić, dlaczego ten okres przechowywania jest niezbędny do danego celu w konkretnych przypadkach. EROD zaleca administratorom, aby zaplanowali możliwie najkrótszy okres przechowywania, również z uwzględnieniem pasażerów, którzy latają bardzo rzadko, i zaoferowali osobom, których dane dotyczą, ustalenie preferowanego okresu przechowywania.

59. W świetle tych rozważań, w odpowiedzi na pytanie 2.1.1, EROD stwierdza, że takie przetwarzanie **można uznać za zasadniczo zgodne z art. 5 ust. 1 lit. e), art. 5 ust. 1 lit. f) oraz art. 25 i 32 RODO, z zastrzeżeniem odpowiednich zabezpieczeń**.

Odpowiednie zabezpieczenia

60. W tego rodzaju scenariuszu, w odpowiedzi na pytanie 2.1.2, EROD uważa, że **oprócz zabezpieczeń wymienionych w scenariuszu 1** należy wdrożyć co najmniej poniżej opisane zabezpieczenia. Zabezpieczenia inne niż te opisane w niniejszej opinii można wykorzystać do osiągnięcia tych samych celów w zakresie bezpieczeństwa i ochrony danych i mogą one być zgodne z prawem, o ile zapewniają zgodność z mającymi zastosowanie ramami prawnymi.

61. Uwaga: *jest to ogólny i niewyczerpujący przegląd możliwych odpowiednich zabezpieczeń, które administrator może wdrożyć w rozwiązaniu podobnym do scenariusza 2. Odpowiedniość zabezpieczeń na podstawie art. 25 i 32 RODO będzie zależała od analizy poszczególnych przypadków. Wszyscy administratorzy będą musieli zapewnić przeprowadzenie własnej oceny skutków dla ochrony danych, a ich konkretne rozwiązania mogą wymagać dodatkowych środków nieuwzględnionych w niniejszej opinii.*

D. Kwestie ogólne

D.1 Prawa osób, których dane dotyczą, i zabezpieczenia, które mogą wdrożyć administratorzy

D.1.1 Należy zapewnić, aby pasażer miał kontrolę nad okresami przechowywania danych w odniesieniu do wszystkich jego danych. Okresy przechowywania powinny być ograniczone do tego, co jest niezbędne do osiągnięcia konkretnego celu. Należy ustalić maksymalny okres na podstawie dogłębnej analizy czynników, takich jak ważność dokumentu identyfikacyjnego. Osobom, których dane dotyczą, należy zaoferować ustalenie preferowanego przez nie okresu przechowywania, który może być krótszy niż domyślny okres przechowywania.

D.1.2 Należy umożliwić osobie, której dane dotyczą, zażądanie w dowolnym momencie usunięcia danych przechowywanych wyłącznie przez nią (klucz dostępu) w aplikacji mobilnej lub cyfrowym portfelu[92].

D.1.3 Należy zapewnić, aby lokalizacja serwera centralnego umożliwiała właściwemu organowi nadzorczemu prowadzenie skutecznego nadzoru.

E. Kwestie organizacyjne:

E.1 Polityka i zgodność

E.1.1 Zaufanie do serwera centralnego musi być ograniczone. Należy zapewnić, aby zarządzanie serwerem centralnym odbywało się zgodnie z jasno określonymi zasadami zarządzania i obejmowało wszystkie środki niezbędne do zapewnienia jego bezpieczeństwa[93].

F. Kwestie techniczne:

F.1 Dostęp

F.1.1 Należy prowadzić ewidencję osób mających dostęp do danych osobowych, w szczególności danych identyfikacyjnych i danych biometrycznych, oraz tego, kiedy uzyskano dostęp do tych danych.

F.2 Infrastruktura i sieć

F.2.1 Należy odpowiednio zabezpieczyć centralną bazę danych, w tym przed atakami na dostępność.

F.2.2 Należy zagwarantować brak połączenia internetowego z centralną bazą danych, bramkami rejestrującymi i jednostkami dopasowującymi. Czynności związane z obsługą i konserwacją tego systemu (np. tworzenie kopii zapasowych, wdrażanie poprawek, monitorowanie itp.) mają być wykonywane lokalnie na terenie portu lotniczego.

F.3 Bezpieczeństwo danych i zarządzanie danymi

[92] Należy mieć na uwadze, że to zabezpieczenie ma zastosowanie wyłącznie do scenariusza 2.
[93] Wytyczne EROD 4/2020 w sprawie danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych, PRYW-5, s. 20.

F.3.1 Należy wdrożyć zgodne z aktualnym stanem wiedzy techniki kryptograficzne w celu zabezpieczenia wymiany informacji między aplikacją a serwerem centralnym[94].

F.3.2 Należy przechowywać osobisty klucz dostępu na poziomie, na którym będzie on wykorzystywany do odszyfrowywania (tj. na czytniku), i wykorzystywać wyłącznie indeks do wyszukiwania odpowiedniego zarejestrowanego wzorca biometrycznego w centralnej bazie danych.

F.3.3 Należy zapewnić, aby udostępnianie klucza dostępu między urządzeniem użytkownika a czytnikiem zabezpieczało komunikację przed ewentualnym podsłuchem lub przesyłaniem do osób trzecich.

F.3.4 Należy zindeksować wzorzec biometryczny przechowywany w centralnej bazie danych, aby umożliwić uwierzytelnianie 1:1 oraz zapewnić jego niepowtarzalny charakter i związek z daną osobą. Należy zapewnić, aby indeks nie ujawniał żadnych danych identyfikacyjnych pasażera i nie był skorelowany z kluczem kryptograficznym.

F.3.5 Należy zapewnić odpowiednie uwierzytelnienie i szyfrowanie wszelkiego przesyłania danych między centralną bazą danych a punktami kontroli oraz dokonywać takiego przesyłania danych w sieciach odizolowanych.

F.3.6 Należy unikać dwukierunkowych połączeń między zbiorami danych (danych identyfikacyjnych i biometrycznych, a także danych dotyczących lotu) i przechowywać w bazie danych wyłącznie odpowiednie połączenia jednokierunkowe. Na przykład tylko jednokierunkowe połączenia od indeksu do danych identyfikacyjnych, od indeksu do zaszyfrowanych danych biometrycznych oraz od indeksu do danych dotyczących lotu.

F.3.7 Należy zapewnić rozwiązania w zakresie ciągłości działania, na przykład poprzez wprowadzenie odpowiednich rezerwowych systemów przechowywania.

F.3.8 Należy zapewnić, aby w czytniku nie były przechowywane ewidencje zaszyfrowanych lub niezaszyfrowanych wzorców.

3.2.3 Scentralizowane przechowywanie zarejestrowanych wzorców biometrycznych do celów identyfikacji

62. W tej sekcji przeanalizowano zgodność z art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO scentralizowanego przechowywania, do celów identyfikacji, zarejestrowanych wzorców biometrycznych pasażerów, w

[94] Wytyczne EROD 4/2020 w sprawie danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych, BEZP-4, s. 18–19: „Do przykładowych technik, które mogą być stosowane, zalicza się: szyfrowanie symetryczne i asymetryczne, funkcje skrótu, test prywatnego członkostwa (ang. *private membership test*), obliczanie części wspólnej zbiorów prywatnych (ang. *private set intersection*), filtry Blooma, odzyskiwanie informacji prywatnych, szyfrowanie homomorficzne".

przypadku gdy takie wzorce nie są zaszyfrowane kluczem, do którego dostęp mają jedynie pasażerowie, w dwóch przypadkach użycia: 1) gdy takie wzorce są przechowywane w bazie danych w porcie lotniczym pod kontrolą operatora portu lotniczego[95] (dalej „**scenariusz 3.1**") oraz 2) gdy takie wzorce są przechowywane w chmurze, pod kontrolą przedsiębiorstwa lotniczego[96] (dalej „**scenariusz 3.2**").

63. EROD uważa, że wykorzystywanie danych biometrycznych do celów **identyfikacji** w dużych centralnych bazach danych koliduje z prawami podstawowymi osób, których dane dotyczą, i może pociągać za sobą poważne konsekwencje dla tych osób[97]. Ponadto wykorzystywanie danych biometrycznych należy przeanalizować również pod kątem celu, w jakim dane te są przetwarzane, w świetle zasad konieczności i proporcjonalności[98].

3.2.3.1 Scenariusz 3.1: scentralizowane przechowywanie w bazie danych w porcie lotniczym pod kontrolą operatora portu lotniczego

Opis scenariusza

64. W scenariuszu 3.1 zarejestrowany wzorzec biometryczny pasażerów jest przechowywany w centralnej bazie danych na terenie portu lotniczego i pod kontrolą operatora portu lotniczego w formie zaszyfrowanej. W szczególności dane pasażerów są kategoryzowane, co oznacza, że dane identyfikacyjne pasażerów, ich zarejestrowane wzorce biometryczne i dane dotyczące lotu są przechowywane w trzech różnych bazach danych. Dane te są szyfrowane różnymi kluczami, zarówno podczas przechowywania, jak i w trakcie przesyłania na serwery dokonujące dopasowania, gdzie zostają następnie odszyfrowane przez operatora portu lotniczego.

65. Pasażerowie muszą zarejestrować się na każdy lot w krótkim czasie przed odlotem (np. 48 godzin). Taką rejestrację można przeprowadzić zdalnie lub w terminalach portu lotniczego z odpowiednim poziomem bezpieczeństwa tożsamości (np. z odpowiednim poziomem bezpieczeństwa zgodnie z rozporządzeniem eIDAS). Alternatywnie rejestracja może mieć taką samą formę, jak opisano w scenariuszu 1, w którym to przypadku pasażerowie muszą przesłać swoje dane ze swoich portfeli cyfrowych do systemu portu lotniczego w ciągu 48 godzin przed odlotem.

66. Również w tym scenariuszu pasażerowie muszą stanąć przed dedykowaną bramką kontrolną wyposażoną w kamerę. Ich wzorzec biometryczny jest następnie przesyłany do centralnego serwera portu lotniczego, który będzie próbował dopasować dane do danych z centralnej bazy danych biometrycznych. Pasażer może zatem zostać zidentyfikowany i zweryfikowany pod kątem tego, czy rzeczywiście jest zarejestrowany na lot odlatujący (lub lot, na który pasażerowie są wpuszczani na pokład, w przypadku kontroli przy wchodzeniu na pokład). W zależności od punktu kontroli dane odesłane do żądającego kontrolera w punkcie kontroli mogą zostać zminimalizowane, na przykład jako „odpowiedź tak/nie" lub, w stosownych przypadkach, jako sam wynik dopasowania. W takim

[95] Ilustruje to przypadek użycia 3A w załączniku I do wniosku.
[96] Ilustruje to przypadek użycia 3B w załączniku I do wniosku.
[97] Zob. na przykład opinia 3/2012 Grupy Roboczej Art. 29 w sprawie technologii biometrycznych, s. 8. Zob. również pkt 26 powyżej.
[98] Motyw 4 RODO. Zob. również opinia 3/2012 Grupy Roboczej Art. 29 w sprawie technologii biometrycznych, s. 8.

przypadku jedynie wynik żądania jest przekazywany kontrolerowi w punkcie kontroli i wykorzystywany przez niego.

67. W szczególności, w tym scenariuszu dokonuje się identyfikacji pasażerów (porównanie 1:N), gdzie N oznacza liczbę pasażerów spodziewaną w porcie lotniczym w ciągu kilku dni. Ponadto dopasowania danych biometrycznych dokonuje się tylko wtedy, gdy każdy pasażer stawia się we wcześniej określonych punktach kontroli w porcie lotniczym odlotu, ale samo przetwarzanie danych odbywa się na centralnym serwerze połączonym z centralną bazą danych. Okres przechowywania w tym scenariuszu wynosi zazwyczaj 48 godzin, a dane są usuwane po odlocie samolotu.

Ocena przeprowadzona przez EROD

68. Jak wspomniano powyżej, przetwarzanie danych biometrycznych pociąga za sobą zwiększone ryzyko dla praw i wolności osób, których dane dotyczą[99]. W związku z tym każda awaria w zakresie bezpieczeństwa danych może mieć szczególnie poważne konsekwencje dla osób, których dane dotyczą[100]. Administratorzy są zobowiązani do skutecznego ograniczania tego ryzyka. Ponieważ w tym scenariuszu cała architektura jest całkowicie scentralizowana, pasażerowie w większym stopniu tracą kontrolę nad swoimi danymi. Ponadto ryzyko, że dane będą przetwarzane w innych celach niż kontrola przepływu pasażerów, może być również większe.

69. W świetle przedmiotowej zasady i wymogów dotyczących bezpieczeństwa (art. 5 ust. 1 lit. f) i art. 32 RODO) należy uznać, że przechowywanie danych identyfikacyjnych i biometrycznych w centralnych, choć odrębnych bazach danych może skutkować punktami ataku o wysokiej wartości, a naruszenie poufności takiej bazy danych może pociągać za sobą dostęp do całego zbioru danych. W związku z tym ewentualne naruszenie dotyczące wzorców rozpoznawania twarzy i powiązanych danych identyfikacyjnych może umożliwić nieupoważnioną lub niezgodną z prawem identyfikację osób, których dane dotyczą, w innych środowiskach. Może również, w zależności od metod stosowanych do identyfikacji biometrycznej, zagrozić dalszemu bezpiecznemu stosowaniu wzorców rozpoznawania twarzy jako identyfikatora. W takim przypadku nie można złagodzić skutków naruszenia, inaczej niż w przypadku innego rodzaju elementu uwierzytelniającego (np. identyfikatora użytkownika, hasła), który można zmienić[101].

70. Ponadto duża ilość i wysoka jakość danych identyfikacyjnych i biometrycznych przechowywanych przez administratora sprawia, że dane te są bardzo cennym celem dla atakującego, co wiąże się z większym prawdopodobieństwem wystąpienia ryzyka dla bezpieczeństwa. Ponadto naruszenia ochrony danych mogą wywoływać większe skutki, ponieważ ze względu na przechowywanie danych w scentralizowanej lokalizacji atakujący mogą łatwiej uzyskać dostęp do danych osobowych dotyczących wielu pasażerów. W związku z tym ewentualne naruszenie mogłoby potencjalnie narazić dużą liczbę osób, których dane dotyczą, na wysokie ryzyko pod względem dotkliwości, na przykład kradzież tożsamości na dużą skalę, które to ryzyko jest niezwykle trudne do ograniczenia.

[99] Zob. pkt 26 powyżej.
[100] Wytyczne dotyczące rozpoznawania twarzy, Komitet Doradczy Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, czerwiec 2021 r., s. 22.
[101] Zob. w tym względzie opinia 3/2012 Grupy Roboczej Art. 29 w sprawie technologii biometrycznych, s. 38.

71. W związku z tym, jeżeli chodzi o zgodność z art. 5 ust. 1 lit. f) i art. 32 RODO, środki przewidziane w scenariuszu 3.1[102], uwzględniając aktualny stan wiedzy, są niewystarczające do zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Na tej podstawie przetwarzanie w ramach scenariusza 3.1 nie byłoby zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO, gdyby administrator ograniczył się do tych środków.

72. W świetle zasady określonej w art. 5 ust. 1 lit. e) RODO w tym scenariuszu okres przechowywania danych biometrycznych w centralnej bazie danych wynosi zazwyczaj 48 godzin. Wydaje się, że takie ograniczenie przechowywania znacznie ogranicza ryzyko związane z naruszeniami ochrony danych osobowych. Niemniej jednak okres przechowywania danych nie jest sam w sobie czynnikiem decydującym o ogólnej kompatybilności wspomnianej architektury, ponieważ takie okresy przechowywania mogą podlegać zmianom ze strony administratorów. W każdym razie proponowane środki muszą być zgodne z wymogami uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych określonymi w art. 25 RODO.

73. W przeciwieństwie do scenariuszy 1 i 2, w których pasażerowie są uwierzytelniani, w scenariuszu 3.1 pasażerowie są identyfikowani (porównanie 1:N), gdzie N oznacza oczekiwaną w porcie lotniczym w ciągu kilku dni liczbę pasażerów, którzy wyrazili zgodę na takie przetwarzanie podczas przechodzenia przez określone punkty kontroli w porcie lotniczym. Wiąże się to z wyszukiwaniem pasażerów w centralnej bazie danych poprzez przetwarzanie każdej pobranej próbki biometrycznej w celu sprawdzenia, czy odpowiada ona osobie znanej systemowi. W przeciwieństwie do scenariusza 2 w scenariuszu 3.1 klucze nie znajdują się wyłącznie w posiadaniu pasażerów. Dlatego też w tym scenariuszu pasażerowie mają znacznie mniejszą kontrolę nad swoimi danymi biometrycznymi. W związku z tym takie przetwarzanie zaproponowane w scenariuszu 3.1 nie jest zgodne z wymogami uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych określonymi w art. 25 RODO.

74. W świetle art. 25 RODO administratorzy muszą uwzględnić rodzaje, kategorie i poziom szczegółowości danych osobowych wymaganych do celów przetwarzania[103]. Dokonując wyborów w zakresie projektowania, powinni oni uwzględnić zwiększone ryzyko dla zasad integralności i poufności, minimalizacji danych i ograniczenia ich przechowywania podczas gromadzenia dużych ilości szczegółowych danych osobowych oraz porównać je z ograniczeniem ryzyka podczas gromadzenia mniejszych ilości lub mniej szczegółowych informacji na temat osób, których dane dotyczą. W żadnym przypadku domyślne ustawienia nie mogą obejmować zbierania danych osobowych, które nie są niezbędne do osiągnięcia konkretnego celu przetwarzania. Innymi słowy, jeżeli określone kategorie danych osobowych są zbędne lub jeżeli szczegółowe dane nie są potrzebne, ponieważ mniej szczegółowe dane są wystarczające, nie powinno się gromadzić żadnych nadmiernych danych osobowych. W takim przypadku, jeżeli inne wdrożenie przetwarzania mogłoby osiągnąć ten sam cel i jest dostępne zgodnie z warunkami opisanymi w scenariuszu 3.1, stosowanie technologii rozpoznawania twarzy nie jest konieczne.

75. W odniesieniu do art. 25 RODO kluczowym elementem uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych jest autonomia osoby, której dane dotyczą. W

[102] Jak opisano w pkt 64–67 powyżej.

[103] Wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, pkt 49.

szczególności należy przyznać osobie, której dane dotyczą, najwyższy zakres autonomii, aby mogła decydować o sposobie wykorzystania jej danych osobowych, a także o zakresie i warunkach tego wykorzystania lub przetwarzania[104]. W scenariuszu 1 osoba, której dane dotyczą, posiadałaby autonomię i kontrolę w zakresie wykorzystywania, ujawniania i usuwania swoich wzorców biometrycznych, a w scenariuszu 2 osoba, której dane dotyczą, zachowałaby pewną kontrolę w odniesieniu do ujawniania własnego wzorca biometrycznego, ponieważ przechowywałaby klucz kryptograficzny. W scenariuszu 3.1 osoba, której dane dotyczą, jest jednak w pełni zależna od decyzji administratora dotyczących przetwarzania jej danych biometrycznych i w związku z tym nie ma bezpośredniej kontroli nad wykorzystaniem jej wzorca biometrycznego.

76. Jeżeli chodzi o zgodność z art. 25 RODO, a w szczególności w celu spełnienia wymogu minimalizacji danych, przetwarzanie przewidziane w scenariuszu 3.1 jest zgodne z zasadą konieczności. EROD uważa, że podobny rezultat usprawnienia przepływu pasażerów w portach lotniczych można osiągnąć w sposób mniej ingerujący w prywatność. Na przykład można to osiągnąć bez wykorzystywania danych biometrycznych (chociaż doświadczenie użytkownika byłoby wówczas inne, ponieważ okazanie karty pokładowej i, w razie potrzeby, oficjalnych dokumentów identyfikacyjnych może trwać dłużej). Ponadto inne rozwiązania, w szczególności rozwiązania oparte na przechowywaniu danych biometrycznych w lokalnym portfelu na urządzeniu osoby fizycznej lub rozwiązania wymagające szyfrowania danych za pomocą konkretnego klucza przechowywanego w urządzeniu osoby fizycznej, umożliwiają osiągnięcie celów w sposób mniej ingerujący w prywatność.

77. Jeżeli chodzi o zasadę proporcjonalności, przetwarzanie przewidziane w scenariuszu 3.1 stwarzałoby ryzyko dla praw osób, których dane dotyczą, którego nie ograniczyłyby przewidziane środki, biorąc pod uwagę aktualny stan wiedzy. Ryzyko negatywnego wpływu na podstawowe prawa i wolności osób, których dane dotyczą, które może wynikać z naruszenia ochrony danych w scentralizowanej bazie danych biometrycznych dużej liczby osób, wydaje się przeważać nad przewidywaną korzyścią wynikającą z przetwarzania, ponieważ taka korzyść jest stosunkowo niewielka, tj. powoduje nieznaczny wzrost wygody i szybkości kontroli. W związku z tym nie uzasadnia to wysokiego stopnia ingerencji tych środków w podstawowe prawa i wolności osób, a przetwarzanie przewidziane w scenariuszu 3.1 nie jest zgodne z zasadą proporcjonalności.

78. W świetle powyższych rozważań, w odpowiedzi na pytanie 2.2.1, EROD stwierdza, że jeżeli przetwarzanie odbywa się w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych, przetwarzanie przewidziane w scenariuszu 3.1:

- **nie może być zgodne z art. 25 RODO**;
- **nie byłoby zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO**, gdyby administrator ograniczył się do środków opisanych w scenariuszu 3.1.

[104] Wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, pkt 70. W motywie 7 RODO wyjaśniono ponadto, że „[o]soby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi".

3.2.3.2 Scenariusz 3.2: scentralizowane przechowywanie w chmurze, pod kontrolą przedsiębiorstwa lotniczego

Opis scenariusza

79. W scenariuszu 3.2 zarejestrowany wzorzec biometryczny pasażerów jest przechowywany w chmurze, pod kontrolą przedsiębiorstwa lotniczego lub jego dostawcy usług w chmurze (podmiot przetwarzający dane). We wniosku określono, że dostawca usług w chmurze miałby siedzibę w EOG[105]. W takim przypadku dane pasażerów są zaszyfrowane, ale zostają odszyfrowane podczas ich użycia (na przykład w momencie przeprowadzania operacji dopasowania), a klucze znajdują się pod kontrolą przedsiębiorstwa lotniczego lub jego podmiotu przetwarzającego świadczącego usługi w chmurze. Dane biometryczne pasażerów są wykorzystywane do identyfikacji pasażerów (porównanie 1:N), gdzie liczba N jest potencjalnie równa liczbie wszystkich klientów przedsiębiorstwa lotniczego[106].

80. Podobnie jak w scenariuszach 1, 2 i 3.1, również w tym scenariuszu pasażerowie muszą się najpierw zarejestrować. W scenariuszu 3.2 rejestracja pasażerów jest jednak przeprowadzana raz, na cały okres, w którym klient posiada konto w przedsiębiorstwie lotniczym. Rejestracja odbywa się albo zdalnie z odpowiednim poziomem bezpieczeństwa tożsamości (np. z odpowiednim poziomem bezpieczeństwa zgodnie z rozporządzeniem eIDAS), albo w terminalach portu lotniczego. Dopasowania danych biometrycznych dokonuje się tylko wtedy, gdy pasażerowie stawiają się we wcześniej określonych punktach kontroli w porcie lotniczym, ale samo przetwarzanie danych odbywa się w chmurze.

81. W porcie lotniczym pasażerowie przechodzą przez dedykowane bramki kontrolne wyposażone w kamerę. Dane biometryczne pasażerów są przesyłane w drodze żądania na serwer w chmurze przedsiębiorstwa lotniczego, gdzie są dopasowywane do danych z centralnej bazy danych. Pasażer może zatem zostać zidentyfikowany i zweryfikowany pod kątem tego, czy rzeczywiście jest zarejestrowany na lot odlatujący (lub lot, na który pasażerowie są wpuszczani na pokład, w przypadku kontroli przy wchodzeniu na pokład).

82. Potencjalnie wyniki dopasowania mogą być udostępniane wielu operatorom portów lotniczych, jeżeli przedsiębiorstwo lotnicze posiada dedykowany terminal lub dostęp do wspólnej infrastruktury systemu informacyjnego portu lotniczego. W zależności od punktu kontroli dane odesłane do żądającego kontrolera w punkcie kontroli mogą zostać zminimalizowane, na przykład jako „odpowiedź tak/nie” lub, w stosownych przypadkach, jako sam wynik dopasowania. W takim przypadku jedynie wynik żądania jest przekazywany kontrolerowi w punkcie kontroli i wykorzystywany przez niego.

83. Okres przechowywania wzorca jest określany przez przedsiębiorstwo lotnicze i może potencjalnie trwać tak długo, jak długo klient posiada konto w przedsiębiorstwie lotniczym.

Ocena przeprowadzona przez EROD

[105] Francuski organ nadzorczy wyjaśnił, że ma to charakter przykładowy i że można również przewidzieć dostawców usług w chmurze, którzy nie mają siedziby w EOG. Ponadto można by również przewidzieć inne rozwiązania w zakresie przechowywania (np. bez korzystania z chmury).

[106] Francuski organ nadzorczy wyjaśnił, że ma to charakter przykładowy i że istnieje rozwiązanie, w którym dane biometryczne są przekazywane za każdym razem przed lotem.

84. Uwagi wyrażone już przez EROD w odniesieniu do scenariusza 3.1[107] mają również zastosowanie do tego scenariusza.

85. Jeżeli chodzi o przedmiotową zasadę i wymogi dotyczące bezpieczeństwa (art. 5 ust. 1 lit. f) i art. 32 RODO), przetwarzanie w scenariuszu 3.2 odbywa się w chmurze i wiele podmiotów może mieć dostęp do tych danych, w tym ewentualnie dostawcy spoza EOG, nawet jeżeli dane są przechowywane w EOG[108]. Taka architektura pociąga za sobą potencjalne ryzyko związane z przekazywaniem danych osobowych do państw trzecich. Ponadto, mimo że dane pasażerów są zaszyfrowane, zostają odszyfrowane podczas ich użycia (na przykład w momencie przeprowadzania operacji dopasowania), a klucze znajdują się pod kontrolą przedsiębiorstwa lotniczego lub jego podmiotu przetwarzającego świadczącego usługi w chmurze. Takie przechowywanie może prowadzić do dalszego zwiększenia obszaru narażenia na ryzyko w zakresie bezpieczeństwa.

86. W związku z tym, jeżeli chodzi o zgodność z art. 5 ust. 1 lit. f) i art. 32 RODO, środki przewidziane w scenariuszu 3.2[109], uwzględniając aktualny stan wiedzy, są niewystarczające do zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Na tej podstawie przetwarzanie w ramach scenariusza 3.2 nie byłoby zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO, gdyby administrator ograniczył się do tych środków.

87. Ponadto w scenariuszu 3.2[110] dane mogą być przechowywane przez długi okres (tj. potencjalnie trwający tak długo, jak długo osoba, której dane dotyczą, posiada konto w przedsiębiorstwie lotniczym). Taki okres przechowywania naraża dane na większe ryzyko naruszenia bezpieczeństwa i wydaje się wykraczać poza to, co jest absolutnie niezbędne i proporcjonalne do celów przetwarzania. EROD zauważa, że okres przechowywania danych nie jest sam w sobie czynnikiem decydującym o ogólnej zgodności wspomnianej architektury z RODO, ponieważ może podlegać zmianom ze strony administratorów danych. Z informacji dostępnych EROD i zawartych w opisie scenariusza 3.2 nie wynika jednak wystarczające uzasadnienie tak długiego okresu przechowywania ani że dostępne są środki, które pozwoliłyby ograniczyć ryzyko dla osób fizycznych. W związku z tym proponowany okres przechowywania nie byłby ograniczony do tego, co jest niezbędne, zgodnie z zasadą ograniczenia przechowywania określoną w art. 5 ust. 1 lit. e) RODO.

88. W każdym razie środki proponowane w scenariuszu 3.2 nie spełniają wymogów uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych określonych w art. 25 RODO. W scenariuszu 3.2 zarejestrowane wzorce biometryczne pasażerów są przechowywane w chmurze, pod kontrolą przedsiębiorstwa lotniczego lub jego dostawcy usług w chmurze (podmiot przetwarzający dane). Jak opisano powyżej, dostęp do tych danych może mieć potencjalnie wiele podmiotów. Ponadto dane biometryczne pasażerów są wykorzystywane do identyfikacji pasażerów (porównanie 1:N), gdzie liczba N jest potencjalnie równa liczbie wszystkich użytkowników/klientów przedsiębiorstwa lotniczego. Taka metoda polega na wyszukaniu osoby z grupy osób w centralnej bazie danych poprzez przetwarzanie każdej uchwyconej twarzy w celu sprawdzenia, czy jest ona zgodna z twarzą osoby znanej systemowi. W przeciwieństwie do scenariusza 3.1 w scenariuszu 3.2

[107] Pkt 68–77 powyżej.
[108] Skoordynowane działanie EROD w zakresie egzekwowania prawa w 2022 r. – korzystanie z usług opartych na chmurze przez sektor publiczny z 17 stycznia 2023 r., s. 19.
[109] Zob. pkt 79–83 powyżej.
[110] Zob. pkt 83 powyżej.

porównanie można przeprowadzić na znacznie większą skalę, ponieważ w tym przypadku kryterium jest liczba wszystkich klientów przedsiębiorstwa lotniczego, natomiast scenariusz 3.1 obejmował jedynie liczbę pasażerów oczekiwaną w ciągu kilku dni.

89. Ponadto, jeżeli chodzi o zgodność z art. 25 RODO, a w szczególności w celu spełnienia wymogu minimalizacji danych, przetwarzanie przewidziane w scenariuszu 3.2 nie jest zgodne z zasadą konieczności. EROD uważa, że podobny rezultat usprawnienia przepływu pasażerów w portach lotniczych można osiągnąć za pomocą innych mniej inwazyjnych środków, na przykład bez wykorzystywania danych biometrycznych, chociaż doświadczenie użytkownika byłoby wówczas inne, ponieważ okazanie dokumentu identyfikacyjnego i karty pokładowej może trwać dłużej. Ponadto inne rozwiązania, w szczególności rozwiązania oparte na przechowywaniu danych biometrycznych w lokalnym portfelu na urządzeniu osoby fizycznej lub rozwiązania wymagające szyfrowania danych za pomocą konkretnego klucza przechowywanego w urządzeniu osoby fizycznej, umożliwiają administratorowi osiągnięcie celów w sposób mniej ingerujący w prywatność.

90. Jeżeli chodzi o zasadę proporcjonalności, przetwarzanie przewidziane w scenariuszu 3.2 stwarzałoby ryzyko dla praw osób, których dane dotyczą, którego nie ograniczyłyby przewidziane zabezpieczenia. Negatywny wpływ na podstawowe prawa i wolności osób, których dane dotyczą, który wynikałby z naruszenia ochrony danych w scentralizowanej bazie danych biometrycznych dużej liczby osób, które to dane są przechowywane w chmurze, wydaje się przeważać nad przewidywaną korzyścią wynikającą z przetwarzania, ponieważ taka korzyść jest stosunkowo niewielka, tj. powoduje nieznaczny wzrost wygody i szybkości kontroli. W związku z tym nie uzasadnia to wysokiego stopnia ingerencji tych środków w podstawowe prawa i wolności osób, a przetwarzania przewidzianego w scenariuszu 3.2 nie można uznać za proporcjonalne.

91. W świetle powyższych rozważań, w odpowiedzi na pytanie 2.3.1, EROD stwierdza, że jeżeli przetwarzanie odbywa się w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych, przetwarzanie przewidziane w scenariuszu 3.2:

- **nie może być zgodne z art. 25 RODO**;
- **nie byłoby zgodne z art. 5 ust. 1 lit. f) i art. 32 RODO**, gdyby administrator ograniczył się do środków opisanych w scenariuszu 3.2;
- **nie byłoby zgodne z art. 5 ust. 1 lit. e) RODO**, ponieważ z dostępnych EROD informacji nie wynika wystarczające uzasadnienie dla okresu przechowywania przewidzianego w scenariuszu 3.2. Aby zapewnić zgodność z zasadą ograniczenia przechowywania określoną w art. 5 ust. 1 lit. e) RODO, administrator musiałby wykazać, że dane osobowe są przechowywane nie dłużej niż jest to niezbędne do celów, w których są przetwarzane.

4 WNIOSKI

92. W odpowiedzi na pytanie 1.1, na podstawie wniosku o wydanie opinii złożonego przez francuski organ nadzorczy, w odniesieniu do wymogów określonych w art. 5 ust. 1 lit. f), art. 25 i 32 RODO oraz na podstawie powyższej analizy, EROD stwierdza, że:

93. wykorzystanie technologii rozpoznawania twarzy do uwierzytelniania za pomocą danych biometrycznych w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych (punkty kontroli bezpieczeństwa, nadawanie bagażu, wchodzenie na pokład i wejście do poczekalni dla pasażerów), można uznać za zasadniczo zgodne z zasadami integralności i poufności

określonymi w art. 5 ust. 1 lit. f), art. 25 i 32 RODO w przypadku architektury przechowywania danych, w której zarejestrowany wzorzec biometryczny każdego pasażera jest przechowywany lokalnie na jego urządzeniu osobistym i pod jego wyłączną kontrolą, z zastrzeżeniem odpowiednich zabezpieczeń opisanych począwszy od pkt 46 powyżej.

94. W odpowiedzi na pytanie 2.1.1, na podstawie wniosku o wydanie opinii złożonego przez francuski organ nadzorczy w odniesieniu do wymogów określonych w art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO, a także na podstawie powyższej analizy, EROD stwierdza, że:

95. wykorzystanie technologii rozpoznawania twarzy do uwierzytelniania za pomocą danych biometrycznych w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych (punkty kontroli bezpieczeństwa, nadawanie bagażu, wchodzenie na pokład i wejście do poczekalni dla pasażerów), można uznać za zasadniczo zgodne z zasadą ograniczenia przechowywania określoną w art. 5 ust. 1 lit. e) oraz z zasadami integralności i poufności określonymi w art. 5 ust. 1 lit. f) oraz art. 25 i 32 RODO w przypadku scentralizowanej architektury przechowywania, w przypadku gdy zarejestrowany wzorzec biometryczny każdego pasażera jest przechowywany w centralnej bazie danych w porcie lotniczym, pod kontrolą operatora portu lotniczego, w formie zaszyfrowanej, do której klucz dostępu posiada jedynie osoba fizyczna, z zastrzeżeniem odpowiednich zabezpieczeń opisanych począwszy od pkt 60 powyżej.

96. W odpowiedzi na pytanie 2.2.1, na podstawie wniosku o wydanie opinii złożonego przez francuski organ nadzorczy w odniesieniu do wymogów określonych w art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO, a także na podstawie powyższej analizy, EROD stwierdza, że:

97. wykorzystanie technologii rozpoznawania twarzy do identyfikacji za pomocą danych biometrycznych w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych (punkty kontroli bezpieczeństwa, nadawanie bagażu, wchodzenie na pokład i wejście do poczekalni dla pasażerów), w przypadku scentralizowanej architektury przechowywania danych, w której zarejestrowane wzorce biometryczne pasażerów nie są zaszyfrowane kluczem znajdującym się jedynie w posiadaniu danego pasażera, w przypadku gdy takie wzorce są przechowywane w bazie danych w porcie lotniczym (pod kontrolą operatora portu lotniczego), nie może być zgodne z art. 25 RODO. Ponadto takie przetwarzanie byłoby niezgodne z zasadami integralności i poufności określonymi w art. 5 ust. 1 lit. f) i art. 32 RODO, gdyby administrator ograniczył się do środków opisanych w scenariuszu 3.1.

98. W odpowiedzi na pytanie 2.3.1, na podstawie wniosku o wydanie opinii złożonego przez francuski organ nadzorczy w odniesieniu do wymogów określonych w art. 5 ust. 1 lit. e) i f) oraz art. 25 i 32 RODO, a także na podstawie powyższej analizy, EROD stwierdza, że:

99. wykorzystanie technologii rozpoznawania twarzy do identyfikacji za pomocą danych biometrycznych w konkretnym celu, jakim jest usprawnienie przepływu pasażerów w portach lotniczych (punkty kontroli bezpieczeństwa, nadawanie bagażu, wchodzenie na pokład i wejście do poczekalni dla pasażerów), w przypadku scentralizowanej architektury przechowywania danych, w której zarejestrowane wzorce biometryczne pasażerów nie są zaszyfrowane kluczem znajdującym się jedynie w posiadaniu danego pasażera, w przypadku gdy takie wzorce są przechowywane w chmurze (pod kontrolą przedsiębiorstwa lotniczego), nie może być zgodne z art. 25 RODO. Ponadto takie przetwarzanie byłoby niezgodne z zasadami integralności i poufności określonymi w art. 5 ust. 1 lit. f) i art. 32 RODO, gdyby administrator ograniczył się do środków opisanych w scenariuszu 3.2. Ponadto z opisu scenariusza 3.2 i informacji, którymi dysponuje EROD, wynika, że przetwarzanie nie byłoby zgodne z zasadą ograniczenia przechowywania określoną w art. 5 ust. 1 lit. e) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Anu Talus)