EDPB Opinion on Facial Recognition Technology at Airports

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

Published in
2024, Vol. 19(2) eucrim
ISSN: 1862-6947
https://eucrim.eu

On 24 May 2024, the European Data Protection Board (EDPB) issued an opinion on the use of facial recognition technology by airport operators and airline companies for biometrically enabled authentication or identification of passengers. The opinion assessed the compatibility of such processing with Art. 5(1)(e) and (f) and Arts. 25 and 32 of the General Data Protection Regulation (GPDR) for the specific purpose of streamlining the passenger flow at airports at four specific checkpoints: security checkpoints, baggage drop-off, boarding, and access to the passenger lounge.

There are four specific scenarios for passenger authentication at the above-mentioned airport checkpoints, which involve the storage of an enrolled biometric template:

- In the hands of the individual, for example, on their individual device, under their sole control in order to authenticate (1:1 comparison) the passenger;
- In centralised storage, within the airport, in encrypted form with a key/secret held solely in the passenger's hands (1:1 comparison). The enrolment could be valid for a given period, for example up to one year after the last flight was taken until the passport expiry date;
- In centralised storage, within the airport, in encrypted form under the airport operator's control (1:N comparison). The storage period in this scenario is typically 48 hours, and the data is deleted once the plane has taken off;
- In centralised storage, in a cloud, in encrypted form under the control of the airline company or its cloud service provider (1:N comparison). The storage period in this scenario could potentially be for as long as the customer holds an account with the airline company.

In its conclusion, the EDPB rejects the last two scenarios as incompatible with Art. 5(1)(e) and (f), and Arts. 25 and 32 GDPR. According to the board, these scenarios go beyond what is strictly necessary and proportionate for processing purposes. Nonetheless, the EDPB holds that the forms of processing envisaged under the first and second scenarios could, in principle, be considered compatible with Arts. 5(1)(e), 5(1)(f), 25, and 32 GDPR, subject to the implementation of appropriate safeguards. Such safeguards should entail, for instance, the following:

- The execution of a Data Processing Impact Assessment (DPIA) by the controllers;
- Accountability and compliance measures;
- Technical safeguards for access, infrastructure and network, data security and management;
- Training and testing.

Safeguards that can be implemented by controllers include, for example, the following:

- Human oversight and intervention to mitigate any biases and ensure that there is no stigmatisation or profiling of passengers though algorithms;
- Transparent processing of data;
- Measures to comply with the purpose limitation principle;
- No capturing of photos or videos from individuals who do not consent to facial recognition and viable alternatives or back-up solutions for such passengers;
- Deletion possibilities.

The EDPB opinion arose from a request by the French Supervisory Authority. Overall, the EDPB recalled that the use of biometric data and in particular facial recognition technology entails heightened risks to data subjects' rights and freedoms.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union