Facial recognition at airports: individuals should have maximum control over biometric data

24 May 2024 EDPB

Brussels, 24 May - During its latest plenary, the EDPB adopted an **Opinion on the use of facial recognition technologies by airport operators and airline companies to streamline the passenger flow at airports***. This Article 64(2) Opinion, following a request from the French Data Protection Authority, addresses a matter of general application and produces effects in more than one Member State.

> **EDPB Chair Anu Talus said:** "More and more airport operators and airline companies around the world are piloting facial recognition systems allowing passengers to go more easily through the various checkpoints. It is important to be aware that biometric data are particularly sensitive and that their processing can create significant risks for individuals. Facial recognition technology can lead to false negatives, bias and discrimination. Misuse of biometric data can also have grave consequences, such as identity fraud or impersonation. Therefore, we urge airline companies and airport operators to opt for less intrusive ways to streamline passenger flows, when possible. In the view of the EDPB, individuals should have maximum control over their own biometric data."

The Opinion analyses the compatibility of the processing with the storage limitation principle (Article 5(1)(e) GDPR), the integrity and confidentiality principle (Article 5(1)((f)) GDPR, data protection by design and default (Article 25 GDPR) and security of processing (Article 32 GPDR). Compliance with other GDPR provisions including regarding the lawfulness of the processing are not in scope of this Opinion.**

There is no uniform legal requirement in the EU for airport operators and airline companies to verify that the name on the passenger's boarding pass matches the name on their identity document, and this may be subject to national laws. Therefore, where no verification of the passengers' identity with an official identity document is required, no such verification with the use of biometrics should be performed, as this would result in an excessive processing of data.
In its Opinion, the EDPB considered the compliance of processing of passengers' biometric data with four different types of storage solutions, ranging from ones that store the biometric data only in the hands of the individual to those which rely on centralised a storage architecture with different modalities. In all cases, only the biometric data of passengers who actively enrol and consent to participate should be processed.

The EDPB found that the only storage solutions which could be compatible with the integrity and confidentiality principle, data protection by design and default and security of processing, are the solutions whereby the biometric data is stored in the hands of the individual or in a central database but with the encryption key solely in their hands. These storage solutions, if implemented with a list of recommended minimum safeguards, are the only modalities which adequately counterbalance the intrusiveness of the processing by offering individuals the greatest control.

The EDPB found that the solutions based on the storage in a centralised database either within the airport or in the cloud, without the encryption keys in the hands of the individual, cannot be compatible with the requirements of data protection by design and default and, if the controller limits themselves to the measures described in the scenarios analysed, would not comply with the requirements of security of processing.

Regarding the principle of storage limitation, controllers need to ensure they have a sufficient justification for the envisaged retention period and limit it to what is necessary for the proposed purpose.

Next, a **report was adopted by the DPAs on the work of the ChatGPT taskforce**. This taskforce was created by the EDPB to promote cooperation between DPAs investigating the chatbot developed by OpenAI.

The report provides preliminary views on certain aspects discussed between DPAs and does not prejudge the analysis that will be made by each DPA in their respective, ongoing investigation***.

It analyses several aspects concerning common interpretation of the applicable GDPR provisions relevant for the various ongoing investigations, such as:

- **lawfulness** of collecting training data ("web scraping"), as well as processing of data for input, output and training of ChatGPT.
- **fairness:** ensuring compliance with the GDPR is a responsibility of OpenAI and not of the data subjects, even when individuals input personal data.
- **transparency and data accuracy:** the controller should provide proper information on the probabilistic nature of ChatGPT's output and refer explicitly to the fact that the generated text may be biased or made up.
- The report points out that it is imperative that **data subjects can exercise their rights** effectively.

Taskforce members also developed a common questionnaire as a possible basis for their exchanges with Open AI, which is published as an annex to the report.

Furthermore, the EDPB decided to develop guidelines on Generative AI, focusing as a first step on data scraping in the context of AI training.

Finally, the EDPB adopted a statement on the Commission's "Financial data access and payments package" (which includes the proposals for the Regulation on the framework for Financial Data Access (FIDA), on the Payments Service Regulation (PSR) and on the Payment Services Directive 3 (PSD3)).
The EDPB takes note of the European Parliament's reports on the FIDA and PSR proposals, but considers that, with regard to the prevention and detection of fraudulent transactions, additional data protection safeguards should be included in the transaction monitoring mechanism of the PSR Proposal. It is important to ensure that the level of interference with the fundamental right to the protection of personal data of persons concerned is necessary and proportionate to the objective of preventing payment fraud.

Note to editors:

** The Opinion has a limited scope and does not examine the use of facial recognition in general and in particular it does not cover the use of facial recognition for security purposes, border control or by law enforcement agencies.*
*** In the request, it is assumed that the processing would be based on each passenger's consent. However, based on the limited scope of the request, the Opinion does not examine the legal basis and in particular the validity of consent for such processing.*

****Until 15 February 2024, OpenAI did not have an establishment in the EU, therefore the one-stop-shop mechanism (OSS) did not apply and each DPA is competent regarding potential infringements that were committed and ended prior to that date. National investigations concerning potential infringements committed prior to February 2024 will continue to be discussed in the taskforce. For infringements continuing or occurring after February 2024, the OSS mechanism applies.*

All documents adopted during the EDPB Plenary are subject to the necessary legal, linguistic and formatting checks and will be made available on the EDPB website once these have been completed.

Artificial intelligence Consistency New Technology Cybersecurity and data breach

Latest news

Facial recognition at airports: individuals should have maximum control over biometric data
24 May 2024 EDPB

EDPB launches French and German versions of its Data Protection Guide for small business
17 May 2024 EDPB

Finnish SA: Administrative fine of € 856,000 for failing to define storage period of customer data

8 May 2024 **Finland**

Czech SA imposed fine of 13.9 million EUR for infringement of Art. 6 and Art. 13 of GDPR

2 May 2024 **Czech Republic**

Hellenic SA: fine on a company for failure to implement technical and organisational measures resulting in unauthorised access by third parties

2 May 2024 **Greece**