

*Alert*

○ Data Law

*Alert*

○ Data Law

*Alert*

○ Data Law

*Alert*

**13** Issue  
2026

Legance

*Italian DPA sanctions airline for GDPR breaches; AGCOM publishes its AI regulatory roadmap*



# The Italian data Protection Authority fines an airline operator for transparency and data retention breaches in relation to passengers requiring special assistance

The Italian Data Protection Authority ("**IDPA**") has imposed a EUR 180,000 fine on an airline operator for breaching Articles 5(1)(a) and (e), 12, and 13 of the GDPR, which came to light during an investigation launched in response to a complaint regarding the processing of **health data of passengers with disabilities or reduced mobility** through the airline's Medical Information for Fitness to Travel or Special Assistance ("**MEDIF**") form.

The MEDIF form is used to collect health information where necessary to assess a passenger's fitness to travel or to arrange medical assistance during the journey.

According to the airline, the form is required only in specific circumstances, such as where passengers require medical assistance during the flight or have particular medical conditions, and is not required where they only need ground assistance.

The complaint originated from a passenger who claimed that she had nevertheless been required to complete the MEDIF form despite not falling within the categories of passengers for whom the airline considered the form to be necessary.

During its investigation, the IDPA consulted the Italian Civil Aviation Authority (ENAC), and concluded that **the processing of health data through the MEDIF form is lawful where necessary to ensure flight safety and provide the assistance required.**

In light of this, as previously stated, the fine was based on separate GDPR infringements identified during the investigation. In particular, the IDPA found that **passengers were not provided with sufficiently clear and comprehensive information regarding the processing of their personal data, including which categories of passengers were actually required to complete the MEDIF form and which sections of the form were mandatory**, either through the airline's website or through the personnel responsible for providing assistance, in violation of Articles 5(1)(a), 12, and 13 of the GDPR.

The IDPA also deemed the **seven-year retention period applied to health data collected via the MEDIF form to be excessive**, holding that such data should be retained only for the period strictly necessary for the organization and completion of the trip, in violation of the provisions of Article 5(1)(e) of the GDPR.

In addition to the administrative fine, the IDPA ordered the airline to revise its privacy information notices, clearly identify the categories of passengers required to complete the MEDIF form and specify which sections of the form are mandatory. The airline was also required to define retention periods that are proportionate to the purposes pursued and to delete data retained beyond the newly established retention limits.

# AGCOM publishes its 2026 Report on Artificial Intelligence: the new regulatory framework between the AI Act, the DSA and fundamental rights

AGCOM (*Autorità per le Garanzie nelle Comunicazioni*, the "**Authority**") has published its 2026 Report on Artificial Intelligence ("**Report**"), setting out the interplay between Regulation (EU) 2024/1689 ("**AI Act**") and the Digital Services Act ("**DSA**"). The Report highlights structural challenges in governance and coordination among national authorities — including AGCOM, AgID and ACN — and signals that certain AI-related transparency obligations are already enforceable under the DSA, irrespective of the pace of AI Act implementation.

For businesses, the key takeaway is that AGCOM, as Italy's Digital Services Coordinator ("**DSC**") under Article 49 of the DSA, has powers to request information, issue injunctions and impose sanctions on hosting providers, online platforms and search engines.

While AGCOM does not have direct competence over AI systems as such (that role falls to AgID and ACN under the AI Act), it can — and intends to — regulate the effects of AI where they intersect with online content dissemination, advertising, user protection, pluralism and disinformation. Businesses deploying Large Language Models (“**LLMs**”) or AI-driven content in these areas should therefore expect AGCOM oversight.

On the regulatory overlap between the AI Act and the DSA, the Report notes that very large online platforms (“**VLOPs**”) and very large online search engines (“**VLOSEs**”) face converging obligations: systemic risk assessments and independent audits under the DSA, plus transparency and labelling requirements for synthetic content under the AI Act. Both frameworks also target manipulative design practices (dark patterns under the DSA; subliminal/manipulative techniques under the AI Act). Given delays in AI Act implementation, the DSA currently serves as the primary enforcement tool for AI-generated content on platforms.

On disinformation and deepfakes, the Report signals heightened enforcement: proposed measures include a 24-hour task force during election campaigns (comprising AGCOM, the Postal Police and platform representatives), protocols for the removal of political deepfakes within two hours, and binding implementation standards for AI content labelling under Article 50 of the AI Act.

From a cross-cutting perspective, the Report's priority recommendations for AGCOM carry significant implications for regulated businesses: these include the establishment of a permanent AI Observatory with public dashboards, the adjustment of the penalty framework to the maximum limits under the DSA (up to 6% of global turnover) and the AI Act (up to 7%), and the testing of regulatory sandboxes for AI systems within AGCOM's areas of competence.

*Alert*

○ Data Law

*Alert*

○ Data Law

*Alert*

○ Data Law

*Alert*

For further information, please contact:

*Andrea Fedi*

afedi@legance.it

*Lucio Scudiero*

lscudiero@legance.it

*Martina Balzani*

mbalzani@legance.it

