PRIVACY RULES

Chiara Agostini

PARTNER AT R&P LEGAL&TAX (ITALY)

RP Legal & Tax

OFFICE

Milano Piazzale Luigi Cadorna, 4
20123 Milano – Italy
T. +39 02 873131
F. +39 02 0287313322
milano@rplt.it

FOCUS AREAS

Advertising - IP & Commercial - Privacy & Data Protection

GET IN TOUCH

Email: chiara.agostini@rplt.it
Mobile: +39 02 87313335
Website: https://www.rplt.it/lang=en

Violation of the confidentiality of medical reports that were visible online even by other patients: the Italian Data Protection Authority sanctions a polyclinic

The data breach

The investigation carried out by the Italian DPA revealed that:

- the data breach originated from a human error occurred during the integration of two different IT systems;
- due to the anomaly,some users were able to view the health data, such as the radiological images associated with identification data and clinical reports, of 74 patients.

According to the Italian DPA, the data controller, allowing users to access to the health data of 74 data subjects, has communicated special categories of data to third parties:

- in violation of the principles of lawfulness, fairness and transparency, as well as integrity and confidentiality of the data processing, pursuant to Article 5, paragraph 1, letters a) and f) of GDPR; and
- in absence of an appropriate legal basis, in violation of Article 9 of GDPR.

The corrective measures adopted by the data controller

According to the data controller's statements, immediately after becoming aware of the data breach, he promptly:

- suspended the service;
- reported the event to his system provider in order to identify the problem and remedy it definitively;
- implemented all the adequate technical and organisational measures to verify whether a data breach occurred;
- informed the Italian DPA.

The sanction

In defining the amount of the fine, the Italian DPA, despite the seriousness of the violation considering the category of personal data involved, has given particular relevance to the high level of cooperation demonstrated by the data controller during the investigation, as well as his timely intervention aimed at promptly removing the damaging effects of the data breach.

Best practices

What arises from this case is that it is essential for data controllers to constantly carry out audits activities
on their suppliers in order to verify and evaluate their work, as well as to have an adequate data breach policy, so they can act promptly and efficiently in the event of an episode of data breach, in accordance with the provisions of Article 33 of the GDPR