Newsletter AUGUST 2021

THE ITALIAN DATA PROTECTION AUTHORITY REITERATES THE NEED TO PROTECT THE IDENTITY OF THE WHISTLEBLOWER THROUGH A SPECIFIC REGIME OF GUARANTEE AND CONFIDENTIALITY

Introduction

On June 10 2021, the Italian data protection authority (the "**Italian DPA**" or the "**Authority**") issued two sanctioning measures in the context of inspections and audits conducted on the personal data processing activities carried out through a system/application ("**Platform**") used to manage whistleblowing reports (the "**Reports**").

In particular, the Italian DPA sanctioned a company and its software provider in SaaS mode, for violation of the applicable laws on the protection of personal data.

Such measures are part of the broader framework of the inspection and control activities of the Italian DPA concerning the management of Reports by data controllers and data processors, in the context of which the Authority had already indicated some elements to pay attention to in order to ensure the compliance of the management of Reports with the applicable laws in the field of personal data protection:

1. the technical functionalities of the Platform must take into account, from its design stage, the applicable principles on the protection of personal data;
2. in particular, the Platform must be equipped with appropriate security measures for the protection of personal data that passes through it and/or is stored on it, including limiting access only to authorized individuals with authentication credentials and a specific authorization profile and the use of encryption techniques;
3. the data controller must, in all cases, adopt appropriate procedures to regularly test, verify and evaluate the effectiveness of the technical and organizational measures put in place (also by third parties) in order to ensure the security of the processing of personal data carried out through the Platform.

Mandatory requirements of the Platform

The above mentioned measures identify the elements which, according to the Italian DPA, are necessary and mandatory in order to ensure compliance with the data protection laws of any Platform through which Reports are submitted and managed:

1. the Platform must be equipped with a secure network protocol (such as the https protocol) to protect the transit of data contained in Reports;
2. suitable data encryption measures must be implemented also with regard to the storage of Reports on the Platform. Failure to use encryption techniques for the transport and storage of data results in a violation of the principle of "accountability", as well as a violation of the obligation of each data controller to adopt adequate security measures to protect the processing activities carried out (as set forth in, respectively, Articles 24 and 32 of Regulation (EU) 2016/679 "**GDPR**");

3. the recording and storage, in specific logs, of the information relating to the connections to the Platform, must not allow the identification of the individuals using the Platform itself, including the reporting parties. Therefore, any tracking mechanism of access to the Platform which allows the recording and storage of accesses to the Platform and/or operations performed through it must be considered in violation of the principle of "minimization" and "privacy by default" (as set forth in, respectively, Articles 5 and 25 of the GDPR);
4. a data protection impact assessment pursuant to Article 35 of the GDPR should be performed on the processing of personal data carried out through the Platform.

Data Controller and Data Processor

In imposing the sanctions in question, the Italian DPA then took the opportunity to state that the provider of the Platform must be considered the "data processor" on behalf of the company purchasing the service for the management of the Reports. In view of this, the data controller is called upon to verify the supplier's compliance with the applicable data protection legislation, providing the latter with specific instructions; the data processor, on the other side, is required to comply with such legislation.

Further considerations

It is also noteworthy that, in the above mentioned measures, the Italian DPA also sanctioned the Platform provider, both for breach of security obligations and for failing to regulate the relationship with two other companies that processed personal data on its behalf, highlighting a number of key points:

1. through the Platform, data belonging to particular categories pursuant to Article 9 of the GDPR and/or data relating to criminal convictions, offences and related security measures pursuant to Article 10 of the GDPR could be processed. In any case, the information passing through the Platform requires special forms of protection, aimed especially at protecting the disclosure of the identity of the reporter and preventing the adoption of discriminatory measures against him/her. Such security measures include:
    a. the encryption of data that pass through and are stored on the Platform;
    b. the use of a defined number of users' credentials (and a ban on users' credentials sharing) to access the Platform;
    c. the use of a "strong" computer authentication procedure;
    d. automatic user blocking mechanisms in the event of repeated failed authentication attempts; etc.
2. the data controller must always have full control over the processing of personal data carried out on its behalf. Therefore, a Platform provider who makes use of other sub-providers in the absence of an agreement or other legal act governing the processing of personal data by the latter, and without the prior authorization of the data controller, is acting in violation of Article 28 of the GDPR.

Final Notes

The elements identified by the Authority open up a useful discussion on the security measures appropriate to ensure the compliance of the processing of data collected through the Reports with the applicable data protection laws, and also offer an opportunity to carry out the appropriate assessments, and identify any remedial actions, necessary to protect the data controllers and data processors from the risk of sanctions.

Newsletter AUGUST 2021

The Data Protection Department of Legance is available to provide any clarifications, also in respect of any specific situation which may be of interest to you.

For further information:

Andrea Fedi

Partner

T. +39 06.93.18.271
afedi@legance.it

Lucio Scudiero

Managing Associate

T. +39 06.93.18.271
lscudiero@legance.it

or your direct contact at Legance.

Newsletter AUGUST 2021

THE FIRM
Legance is an independent Italian law firm with expert, active and result-oriented lawyers, with a strong team spirit that has permitted a flexible and incisive organisational model that, through departments active in all practice areas of business law, offers the right balance between the specialist and the lawyer as a global consultant. Legance comprises over 280 lawyers, working in its Milan, Rome, London and New York offices, and has a diverse and extensive practice covering the following areas: Administrative; Banking & Finance; Compliance; Corporate Finance; Data Protection; Debt Capital Markets; Dispute Resolution; Employment and Industrial Relations; Energy, Project & Infrastructure; Environmental; Equity Capital Markets; EU, Antitrust and Regulation; Financial Intermediaries Regulations; Food; Insurance; Intellectual Property; Investment Funds; Life Sciences & Healthcare; Non Performing Loans; Real Estate; Restructuring and Insolvency; Shipping, Aviation and Transportation; Tax; Telecommunications, Media and Technology; White Collar Crimes. For more information, please visit our website: www.legance.com.