CONTRIBUTOR

ARTICLE

Italy: Relationship Between EU Regulation 679/2016 (GDPR) And Legislative Decree 231 Of 2001 Risk Based Methodological Approach And Risk Assessment

22 July 2021

by Nicolò Ghibellini (Bergamo)

Marazzi & Associati

The purpose of this brief contribution is to highlight the possible points of contact between the discipline dictated by the GDPR and that of Legislative Decree 231 of 2001.

First of all, it may be useful to recall that Regulation 679/16 EU (the GDPR) is the legislation that since 2018 (year of its effective applicability) governs the protection of personal data. Fundamental principles of the GDPR are the accountability of the Data Controller, privacy by design and by default, the assessment of risks associated with data processing and the consequent implementation of technical and organizational measures for the minimization of these risks.

Legislative Decree 231/2001 - Regulations governing the administrative liability of legal entities, companies and associations, including those without legal personality - introduced into the Italian legal system a system of administrative liability dependent on the commission of certain offences by companies.

In general, it can be observed that a first point of contact between the two regulations is represented by the circumstance that both are based on the analysis of internal processes, on the definition of an organizational model that represents it, as well as on the analysis of related risks. More specifically, we identify the following adherences between the two aforementioned disciplines.

a) Art. 5.2 and 24 GDPR and art. 6 Legislative Decree 231/01

It follows from the combined provisions of Articles 5.2 and 24 of the Regulation, that taking into account the nature, scope, context and purposes of the processing, as well as the risks having different probability of occurrence and severity of consequences for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure, and be able to demonstrate, that the processing is carried out in accordance with the Regulation. These measures shall be reviewed and updated as necessary.

In essence, therefore, the Data Controller must not limit himself to following the regulations in a "bureaucratic" manner, as a list of measures to be adopted, but has the possibility and the responsibility to decide and choose the means that he considers most appropriate to achieve the purposes established by the Regulations. The firm must also be able to assess the status of its own accountability and the appropriateness of its own actions, in order to be accountable to the relevant authorities.

Similarly, Art. 6 of Legislative Decree 231/01 provides that the entity is liable for the unlawful act committed by persons operating within it if it does not prove the adoption and effective implementation of the Organizational Model. Therefore, in both cases, the sector legislation requires the adoption of organizational measures/models that make the obliged parties virtuous and compliant.

b) Management systems based on the definition of the "chain of command".

The efficiency of the privacy management system requires the definition of an organic and clear hierarchical structure outlined by the Data Controller to which the strategic choices underlying data processing are entrusted; in this context the key roles are, in addition to the Data Controller, any internal contacts, the persons in charge, the managers (sub managers ex art. 28 GDPR) and the Data Protection Officer.

In the 231 context we speak of Segregation of Duties to express the principle that ensures the traceability and transparency of business processes exposed to the risk of verification. This principle is at the basis of the elaboration of company procedures which constitute (together with risk assessment) the heart of the organizational model.

c) Risk assessment and prevention measures

Risk analysis is at the heart of any management system as it is an essential prerequisite for the drafting of organised Privacy and 231 models. In the field of privacy, the above-mentioned is realized in the identification of the level of risk for each treatment (both at the level of physical infrastructure and IT) and in the consequent adoption of appropriate security measures in practice (the concept of minimum measure has disappeared from the GDPR), such as information, training, various policies (use of computer systems, data breach, etc.). In the context of 231 we talk about the analysis of business activities exposed to the risk of commission of offences (so-called sensitive activities) and in Gap Analysis, which must lead - also here as a practical/operational consequence - to the adoption of measures and control tools suitable to prevent the crimes abstractly achievable in the business context of reference, such as the Code of Ethics, Protocols / operating procedures in relation to sensitive activities (financial flows, management inspections, information flows to the SB).

Ultimately, therefore, the GDPR and Legislative Decree 231/01 have many similarities in their approach and this implies that the two models, although they cannot overlap, must communicate with each other, also in order to improve their adherence to the reality in which they operate.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

AUTHOR(S)

Nicolò Ghibellini
Marazzi &
Associati