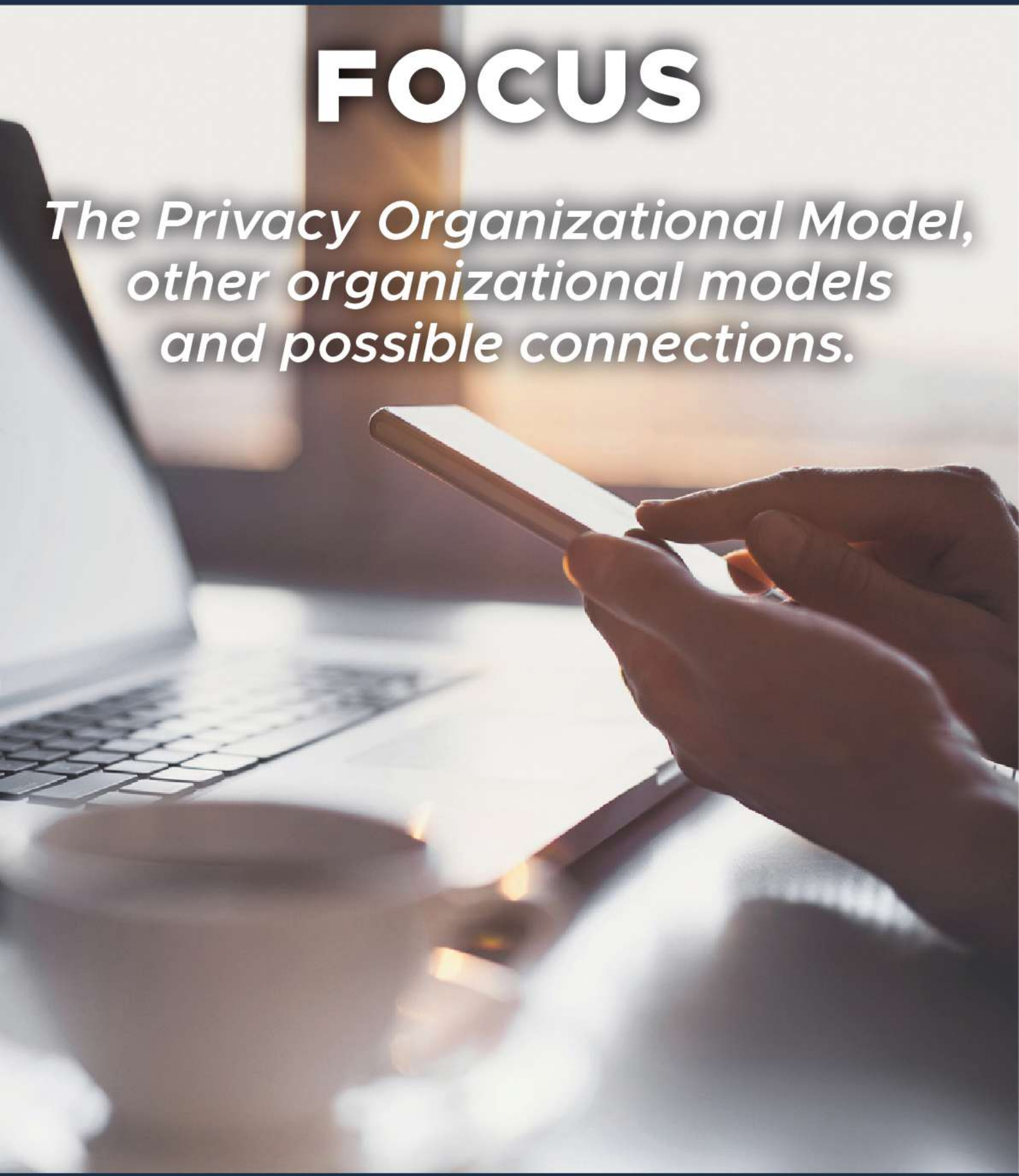
FORNARI E ASSOCIATI
STUDIO LEGALE

FOCUS

The Privacy Organizational Model, other organizational models and possible connections.



fornarieassociati.com

Milan • Rome • Bari

April 2023

I. INTRODUCTION.

The protection of natural persons with regard to the processing of personal data[1] is a fundamental right enshrined in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union, which states that every person has the right to the protection of personal data concerning him or her.

As provided for in Regulation (EU) No. 2016/679 (hereinafter, the "**GDPR**" or the "**Regulation**") – in force since May 24, 2016 – the principles and rules protecting individuals with regard to the processing of personal data[2] should respect their fundamental rights and freedoms, regardless of their nationality and residence.

Through the GPDR, which became fully applicable as of May 25, 2018, the European Commission's objective was to ensure a consistent and high level of protection of personal data of all natural persons present on the territory of the European Union, giving citizens control over their personal data, simplifying the regulatory environment, and unifying the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data in all Member States.

In order to harmonize the rules provided by the Italian legislator within Legislative Decree No. 196/2003 (hereinafter, the "**Privacy Code**"), on September 4, 2018, Legislative Decree No. 101/2018 was published in the Italian Official Gazette, bringing national legislation in line with the GDPR.

Among the general principles applicable to data processing, in Article 5(2), the GDPR emphasizes the so-called principle of accountability of the Data Controller[3] (hereinafter also the "**Data Controller**"), who must not only comply with the criteria set forth in Article 5[4], but must be able to adopt proactive behaviors, such as to demonstrate

1 Pursuant to Article 4(1)(2) of the GDPR, processing is: "*any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, comparison or interconnection, restriction, erasure or destruction*".

2 According to Article 4(1)(1) of the GDPR, personal data is: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by reference in particular to an identifier such as a name, an identification number, location data, an online identifier, or to one or more characteristic features of his or her physical, physiological, genetic, mental, economic, cultural or social identity*".

3 According to Article 4, paragraph 1, number 7) of the GDPR, the Data Controller is: *"the natural or legal person, public authority, service or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria applicable to its designation may be established by Union or Member State law*".

4 In addition to the pillar of "accountability" the applicable principles under Article 5 of the GDPR are (i) lawfulness, fairness, and transparency; (ii) purpose limitation; (iii) data minimization; (iv) accuracy; (v) retention limitation; and (vi) integrity and confidentiality.

the concrete implementation of measures aimed at ensuring the application of the aforementioned Regulation (see Article 24 GDPR).

In this regard, among the measures considered most appropriate and effective in terms of accountability, the adoption of the Privacy Organizational Model (hereinafter, "MOP") is considered to be one of them. This is the document whose primary purpose is to provide evidence of the actions put in place by an organization to address data protection compliance.

II. Is the MOP a valid accountability measure with respect to the GDPR?

As explained above, in the path to GDPR compliance, it is necessary to identify and adopt the most appropriate tools and measures to ensure that the processing of personal data takes place in accordance with the conditions prescribed by Article 5 of the Regulation.

At the same time, the GDPR also imposes an obligation on the Data Controller to demonstrate – upon request – that appropriate and effective measures have been taken. In fact, the provision in Article 5 of the GDPR is echoed by Recital 74, which, consistent with the aforementioned Article 24 GDPR, provides that "*the data controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with this Regulation, including the effectiveness of the measures* [...]," and that this ability to demonstrate compliance with the requirements set forth in the GDPR must persist at every stage of the compliance journey.

By expressly recalling accountability, a cardinal principle of the GDPR, the European Legislator requires the Data Controller to envisage, prepare and adopt technical and organizational measures deemed appropriate to manage the processing activities in such a way as to protect the rights and freedoms of the data subjects, in accordance with the regulations and principles of the GDPR and, above all, to be able to concretely demonstrate at all times the effectiveness of such measures.

That said, although not expressly required by the GDPR, it is believed that the MOP, having the objective of bringing together in a single document all the activities put in place in compliance with privacy regulations, the rationale behind the choices related to data processing as well as the timetable for compliance, can represent an effective accountability measure for business organizations. Obviously, it is of paramount importance that this document be constantly updated as contextual changes impact the subject matter.

III. Specifically, what is the purpose of adopting a MOP?

The MOP represents a specific practical tool that allows the Owner, depending on its organization, the responsible and autonomous choice and management of data protection compliance.

At the same time, this act makes it possible to document and demonstrate at all times:

- compliance with the fundamental principles established by the GDPR;
- the compliance of the processing carried out with the GDPR;
- the effectiveness of the best measures chosen and adopted in the processing activities;
- the continuity over time of the compliance path undertaken, even in the face of any changes in the company's organizational structure;
- of having undertaken a well-structured and defined compliance path, capable of also providing the supervisory authorities with the necessary coordinates in carrying out controls and audits.

Obviously, there is no single, exhaustive model suitable for every entity; rather, the document will have to be calibrated according to the peculiarities of individual business organizations (both the internal context, see the type of data processed, and the external context, such as the measures imposed by external parties such as Data Controllers), through a tailor-made method.

To properly structure a MOP, reference should be made to Recital 74 and Article 24 of the GDPR, which provide guidelines for the adoption of appropriate and effective technical and organizational measures.

In particular, it will be necessary to take into account:

- the nature of the processing;
- the scope of application;
- the context of the processing;
- the purposes of the processing;
- the risks having different probability and severity for the rights and freedoms of natural persons;
- the state of the art and the cost of implementing appropriate measures for the protection of personal data, and the scope of the processing (as indicated by Article 25 GDPR).

In particular, Article 25 GDPR introduces essential principles on the basis of which to properly delineate an MOP: these are the principles of privacy by design and privacy by default, namely "data protection by design" and "data protection by default."

Depending on the GDPR's risk assessment-focused approach, the aforementioned principles require the Data Controller or the Data Processor[5] (hereinafter also the "Processor") – both when determining the means of processing and at the time of processing itself – to put in place appropriate technical and organizational measures designed to effectively implement the data protection principles, and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects.

In essence, the primary purpose of the MOP is to condense into a single text, for the benefit of all stakeholders, a series of documents that might otherwise be difficult to inventory and monitor, especially for medium- to large-sized companies in which documentation pertaining to data protection tends to proliferate.

5 According to Article 4(1)(8) of the GDPR, the Data Processor is: "*the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller*".

IV. How is the MOP structured?

It has been said that through the MOP, the organization concerned can systematically order all the procedures and measures adopted and those to be implemented in the privacy compliance journey, with the relevant documentation.

In practice, the MOP may be structured to account for and collect in systematic order:

- the regulatory provisions that govern the organization's privacy sector. In fact, the MOP contains or refers to procedures, instructions, templates and other documents that the organization may have prepared to give evidence of the application of the regulations. This is in deference to one of the fundamental principles of management systems documentation, which requires that texts having the same content in different documents should not be duplicated. The component parts of the MOP, in turn, can be used as audit criteria;
- the definition of basic privacy principles and terms in relation to the nature of the processing carried out;
- the description of the organization and the type of personal data processing. As anticipated, the MOP should be updated when there are changes in the context (internal or external to the organization), when there are regulatory updates, when new measures are introduced, or when measures are modified or eliminated that are deemed no longer appropriate. A history of the different versions of the document should be kept in order to understand its evolution over time;
- the mapping of information flows and the type of data processed;
- the organization chart of the Data Controller;
- the disclosures (e.g., privacy notices for clients, staff, suppliers, external users, or processing consent templates);
- the roles, functions and responsibilities of the Data Controller, as well as the individuals delegated to process personal data;
- the contractual relationships between the Owner, co-owners, Data Processors and, if appointed, the Data Protection Officer (hereinafter "**DPO**[6]") and their responsibilities;
- the acts of appointment of the internal authorized persons in charge of processing, with the relevant powers, duties, roles and responsibilities (ex Articles 2-quaterdecies of the Privacy Code and 29 of the GDPR);
- staff training activities, setting up a system to document the training carried out for each individual (Art. 39 of the GDPR);
- internal staff behavior procedures and policies for the use of electronic systems and devices, e-mail, internet, and electronic filing systems;

---

[6] Pursuant to Art. 37(1) of the GDPR: "*The controller and the processor shall systematically designate a data protection officer whenever: (a) processing is carried out by a public authority or a public body, with the exception of judicial authorities when exercising their judicial functions; (b) the main activities of the controller or processor consist of processing operations which, by their nature, scope and/or purposes, require the regular and systematic monitoring of data subjects on a large scale or (c) the principal activities of the controller or processor consist of processing, on a large scale, special categories of personal data referred to in Article 9 or data relating to criminal convictions and offenses referred to in Article 10*".

- the audit procedures for verifying compliance with the GDPR;
- the assessment of technical and organizational measures to ensure levels of security appropriate to the risk (Art. 32(2) GDPR);
- the documentation pertaining to the review, updates and implementation of the adopted technical and organizational measures;
- the risk assessment ("**Risk Assessment**") procedure under Art. 32(2) GDPR, and the impact assessment procedure (so-called "DPIA") of planned data protection processing in the presence of high risks to the rights and freedoms of data subjects;
- the operational practices in the event of data breaches (so-called "**Data Breach**"[7]) and security incidents for both its own organization and any data controllers and/or co-processors;
- the procedures for the exercise of data subjects' rights;
- the templates for notification to the Guarantor ex art. 33 in case of Data Breach and communication to data subjects ex art. 34 GDPR, as well as the template for requesting the exercise of data subjects' rights and feedback from the organization;
- the adoption of codes of conduct and/or organizational models pursuant to Legislative Decree no. 231/2001;
- company certifications.

In the case of a group of companies, the MOP is also concerned with clarifying and defining (i) the role and responsibilities of the individual companies within the group; (ii) the internal and holding company relationships; (iii) the modalities of data transfer between the individual entities; and (iv) the purposes of the processing carried out by each entity.

V. WHICH ARE THE RECIPIENTS OF THE MOP?

The recipients of the MOP are:

- the DPO (when present);
- the Data Controller, in case the organization – which prepared the MOP – plays the role of the Responsible Party (in that case, the latter should be allowed only partial access to the MOP);
- the persons in charge of the audit/inspection activity;
- those authorized to process (again, only partial access to the document may be allowed);
- any other individuals representing interested parties.

Access to the document must, in all cases, be authorized by the organization's management.

Regarding the individuals involved, the MOP is usually drafted by the Privacy Contact or Privacy Officer and approved by the Data Controller. When a DPO is designated, the DPO makes an assessment of the document, requesting amendments and additions as appropriate.

7 Pursuant to Article 33(1) of the GDPR: "*In the event of a personal data breach, the data controller shall notify the breach to the competent supervisory authority in accordance with Article 55 without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay*".

VI. ARE THERE STANDARDS TO BE MET FOR THE PURPOSE OF MOP DRAFTING?

When drafting the MOP, it is also useful to take into account the standards provided by ISO standards, in particular ISO/IEC 27701, for personal information management and privacy (which updated previous standards such as ISO/ IEC 27001:2017 and ISO/IEC 27002), aimed at providing a practical tool for organizations to (i) implement the personal information management and security system; (ii) document the technical and organizational choices made; (iii) improve internal controls and audits; and (iv) coordinate with supervisory authorities for appropriate audits.

As an alternative to the aforementioned standard, the other possible (and viable) option is to look at the best practices indicated by ISO 29100, aimed at defining an operating manual in privacy, published in 2011 and updated in 2015.

In any case, regardless of whether or not the standards described above are incorporated, it remains essential that the MOP encapsulates all privacy compliance activities put in place and to be implemented, as well as that the document be updated frequently.

VII. WHAT ARE THE ADVANTAGES OF ADOPTING THE MOP?

In order for the MOP to reveal its usefulness on the organizational level as well, the same must be brought to the attention of all subjects – operating within the organization – involved in personal data processing activities, together with the documentation elaborated in the field of privacy.

In particular, these documents must be usable and viewable by all employees and collaborators in order to improve coordination and dialogue between the different corporate functions, allowing to maintain a constant path of adaptation even in the case of changes in the corporate organization.

The adoption of a MOP, as already mentioned, also enables the organization to comply with the duty to cooperate with the supervisory authorities in inspections and in the performance of their duties, as expressly stipulated in Articles 30(4) and 31 of the GDPR.

The MOP thus represents for organizations that process personal data, along with the register of processing activities[8] and the Data Breach Register, a key tool for implementing the GDPR.

Finally, the greatest utility that can accrue to an organization comes from its ability to make all the organizational models it has adopted talk to each other. In this sense, the MOP can be the point of reference and connection for all previously adopted organizational models, representing the processing of personal data as an activity that cuts across every business sector.

8 According to Article 30(1) of the GDPR: "*Each data controller and, where applicable, its representative shall keep a register of the processing activities carried out under its responsibility*".

VIII. WHICH ARE THE POINTS OF CONTACT BETWEEN THE MOP AND MODEL 231?

Speaking of MOP immediately calls to mind the Organization Model referred to in Legislative Decree No. 231/2001 (hereinafter "**Model 231**").

As is well known, Legislative Decree No. 231/2001 regulates the liability of entities for administrative offenses dependent on crime and allows for the elimination or mitigation of the risk and consequences of the burdensome penalties associated with the commission of particular crimes (so-called "**Predicate Offence**"), similarly to Article 30 of Legislative Decree No. 81/2008 ("Consolidated Law on the Protection of Health and Safety in the Workplace"). In fact, the aforementioned Law also provides for the possibility of establishing a suitable organization and management model with exempting efficacy of the entity's administrative liability in the case of occupational health and safety crimes.

The adoption of Model 231 is therefore a very important defensive element for the defense of corporate organizations in criminal trials in which the entity is found to be a defendant, provided that the Model 231 concretely adopted is suitable "*to prevent crimes of the kind that have occurred*"[9].

Unlike the provisions of Legislative Decree No. 231/2001, the GDPR is not built around a specific organizational model and therefore does not provide for a mandatory minimum content.

Nonetheless, some of the requirements of the GDPR find their correspondence or similarity with those that represent the minimum content of the 231 Model under Articles 6 and 7 of Legislative Decree No. 231/2001:

- identify the personal data processing activities that are most at risk of breaches and carry out an impact assessment on the processing when it presents high risks for the rights and freedoms of the individuals involved (Art. 35 GDPR – see Art. 6, paragraph 2, letter A, Legislative Decree No. 231/2001);

- provide for and plan training measures to ensure that those acting under the Controller (or Manager) are adequately instructed so that processing is carried out in accordance with the GDPR and guarantees the protection of the rights of the data subjects (art. 29 GDPR – see art. 6, paragraph 2, lett. B and D, Legislative Decree no. 231/2001);

- put in place appropriate technical and organizational measures both to effectively implement the principles of data protection "by design" and "by default," also taking into account the costs of implementation, and to ensure a level of security appropriate to the risk (Articles 25 and 32 GDPR – see Art. 6, paragraph 2, lett. C, Legislative Decree no. 231/2001);

- once a possible breach of personal data of data subjects has been discovered, take measures to avert the occurrence of a high risk to the rights and freedoms of data subjects even after the occurrence of

[9] Art. 6 Legislative Decree no. 231/2001.

a Data Breach by reviewing and implementing the measures taken (Art. 34 GDPR – see Art. 7, paragraph 4, Legislative Decree No. 231/2001);

- proceed to the review of the data protection impact assessment when changes in risk arise in processing activities (Art. 35 GDPR – see Art. 7, paragraph 4, Legislative Decree No. 231/2001);

- proceed to review and update the adopted technical and organizational measures when necessary, as well as to supplement the necessary safeguards to meet the requirements of the GDPR even in the course of processing (Art. 35 GDPR – see Art. 7, paragraph 4, Legislative Decree No. 231/2001).

In addition, both models are built on an approach based on risk assessment, placing the principle of empowerment of the organization at the center, and provide for the possibility of referring to codes of conduct to demonstrate compliance with reference regulations (Art. 32 GDPR and Art. 6 Legislative Decree no. 231/2001).

Not only that, of course, both documents must be constructed on the basis of the peculiar characteristics of each business reality, in a path of constant adaptation that also takes into account the evolution of the organization.

Finally, both models – though for different purposes – are aimed at preventing the risk of unlawful processing of personal data. On the one hand, the control system envisaged by Legislative Decree No. 231/2001 is aimed at preventing crimes in the interest or to the advantage of the organization, including computer crimes and the unlawful processing of data among the Presumed Crimes (Art. 24-bis Legislative Decree no. 231/2001); on the other hand, the GDPR aims to protect the fundamental rights and freedoms of the data subjects.

However, the models differ mainly in that with the prior adoption of an effective Model 231, the entity can, in addition to preventing, exclude its liability for crimes committed by members of its organization.

Conversely, the adoption of an MOP does not in itself allow the organization to exclude its liability for Data Breach and/or non-compliance with the principles and rules of the GDPR.

IX. Are there connections between the MOP, other models and other management systems?

Integration between standards and systems is a hot topic, to which specific standards such as the recent ISO 37301:2021 "*Compliance management systems - Requirements with guidance for use*" are dedicated, which provides the "*Guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization*".

The MOP by its very nature tends to foster integration, for the benefit of all stakeholders, to manage personal data in the most efficient way, while complying with internal regulations and procedures.

In fact, the document contains or recalls procedures prepared to document business processes, also taking into consideration privacy implications.

The following are examples of management system integration:

- the procedure on e-waste management impacts the issues of environment, information security and personal data protection (in this regard, the reference standards are represented by Legislative Decree no. 49/2014, UNI EN ISO 14001:2015; ISO/IEC 27001:2022 and GDPR);

- the procedure on the management of accidents concerns issues involving the health and safety of workers and the protection of personal data (in this regard, the reference standards are given by Legislative Decree no. 81/2008, UNI ISO 45001:2018 and the GDPR);

- the procedure for the evaluation of suppliers takes into consideration (i) the ability to provide a service/product in line with business needs; (ii) performance monitoring; (iii) the guarantees provided in the role of Data Processors (in this regard, the reference standards are UNI EN ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019 and the GDPR).

X. What are the benefits of an integrated management system?

The goal of integration is to condense all aspects pertaining to business processes into a limited number of documents to ensure their organic management, avoiding duplication of rules that might partly overlap or risk contradiction. In other words, therefore, the integrated management system makes it possible to avoid duplication of procedures among several systems and to prevent or eliminate possible conflicts between regulations.

In addition to document uniqueness, adopting an integrated system makes it possible to:

- create synergies between business processes that cut across the business organization;
- unify corporate objectives;
- simplify relationships between business functions;
- assess and thus prevent business risks according to a unified approach.

CONTACTS

Giuseppe Fornari
Founder Partner

g.fornari@fornarieassociati.com

Pasquale Grella
Of Counsel

p.grella@fornarieassociati.com

Caterina Peroni
Associate

c.peroni@fornarieassociati.com

Milan
Via Chiossetto 18
P: +39 0254122206
E: milano@fornarieassociati.com

Rome
Piazza di San Lorenzo in Lucina 26
P: +39 0622201000
E: roma@fornarieassociati.com

Bari
Via Principe Amedeo 25
P: +39 0809184280
E: bari@fornarieassociati.com