GDPR: EU REGULATION 2016/679

GDPR

(General Data Protection Regulation)

EU 2016/679

The DPO of EU

Regulation 2016/679

HOW TO PROCEED

for a GDPR Privacy Plan

The new European Regulation (EU) 2016/679 for GDPR Data Protection (General DataProtection Regulation) determines the "guidelines" to be adopted on the subject Protection of Natural Persons with regard to the Processing of Data as well as the free movement of such data.

It is important to underline the fact that, although the obligation is for all companies, the "Data" to which the Regulation refers are those that lead back or that can in some way be traced back to Natural Persons and not legal entities (companies).

With the European regulation on the protection of personal data (regulation 2016/679), approved on 14 April 2016 by the European Parliament and published in the Official Journal of the European Union on 4 May 2016, a new season begins for the rights of European citizens.

The regulation is a valuable attempt to harmonize the privacy rules of the various states and is aimed at developing the digital single market through the creation and promotion of new services, applications, platforms and software.

The Regulation constitutes with Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, the so-called "personal data protection package".

The ADVANTAGES of the New EU Regulation 2016/679 or GDPR

With this Regulation, the European Council, in addition to harmonizing and updating privacy regulations throughout the EU, has as its second objective, to redefine the approach of companies in the field of data protection, by virtue of the continuous cyber attacks to which companies of all sizes and sectors have been subject for some years, providing useful guidance in this direction as well.

The main advantages of the GDPR are:

• single rules for the whole EU
• A level playing field for all EU companies
• rules suitable for the web-economy
• "scalable" and "adaptable" rules to technological changes and future economic scenarios.

The main novelty of the new regulation is that the concept of "MINIMUM MEASURES", at the basis of the current legislation Legislative Decree 196, disappears to give way to that of "ADEQUATE MEASURES".

But the real revolution is the introduction of the new principle of "ACCOUNTABILITY".

This factual principle gives more discretion but, at the same time, greater discretio and responsibility to the "Data Controller" on everything related to data protection with a substantial increase in the penalties provided for in the event of non-compliance.

Citizens, with the new provisions, are at the center of the system; citizens are recognized: the right to data portability, the right to be forgotten, the right to be informed in a transparent, loyal and dynamic manner about the processing carried out on your data and to control, the right to be informed about breaches of your personal.

Citizens shall have the right to give a mandate to a non-profit-making body, organisation or association, duly constituted in accordance with the law of a Member State, the statutory objectives of which are in the public interest and active in the field of the protection of the rights and freedoms of data subjects with regard to the protection of personal data, to lodge a complaint on their behalf and to exercise their rights on their behalf (see Appendix Review, Arts. 77, 78 and 79) as well as the right to obtain compensation for damage caused by the infringement of the regulation.

With the new text of the regulation on the protection of personal data, the "principle of accountability" (reporting obligation) enters our legal system:

- *the public administrations responsible for data processing must demonstrate;*
- *that it has adopted adequate and effective security measures to protect data and that its activities are constantly reviewed and updated;*
- *processing operations comply with the principles and provisions of the European Regulation, including the effectiveness of the measures.*

The regulation provides that adherence to codes of conduct (see Article 40) or to a certification mechanism (see Article 42) can be used as an element to demonstrate compliance with the obligations of the data controller (other elements of strong innovation compared to the previous legislation).

In order to be able to demonstrate compliance with the provisions of the regulation, the obligation of the owner or manager to keep a register of the processing activities carried out under his or her responsibility with a description of the security measures is provided for (art. 30).

The Regulation specifies that the register must contain a general description of the technical and organisational security measures and that upon request, the controller or processor and, where applicable, the representative of the controller or processor are obliged to make the register available to the authority.

The DPO of EU Regulation 2016/679

The regulation introduces a new, the "data protection officer" that public administrations are obliged to appoint internally and must always be "involved in all matters concerning the protection of personal data".

The data protection officer (DPO) must possess specific requirements: competence, experience, independence and autonomy of resources, absence of conflicts of interest and must oversee the organisational privacy profiles through surveillance work on the correct application of the European regulation, privacy legislation and internal legislation, on the attribution of responsibilities, information, awareness and training of personnel, information, advice and issuing opinions.

The data protection officer, who may be both internal and external to the entity, will be required to oversee the privacy profiles, cooperate with the Guarantor Authority and report directly to the top management of the data controller.

The Data Protection Officer is a point of reference and contact for citizens who can contact them for all questions relating to the processing of their personal data and the exercise of their rights deriving from the European regulation. The identity and contact details of the data protection officer must be reported, with a view to transparency towards citizens, in the privacy policy to be provided before the provision of data by citizens, must be published on the website of the entity (art.37) and also contained in the register of processing.

In carrying out his or her duties, the data protection officer shall duly consider the risks inherent in the processing, taking into account the nature, scope, context and purposes of the processing.

The text also provides for a strengthening of the powers of the national Supervisory Authorities and a tightening of administrative sanctions against companies and public administrations: in the case of violations of the principles and provisions of the regulation, the penalties, in special cases, can reach up to 10 million euros or for companies up to 2%-4% of the total annual worldwide turnover of the previous year, if higher.

HOW TO PROCEED for a GDPR Privacy Plan

1.Laying the FOUNDATIONS

In this FIRST PHASE it is important to involve, in addition to the Managers, also the Key Users who are responsible for the various processes and departments that will most intervene in the project.

2.Map data and do gap analysis

In this it is important to detect and document what personal data is in the possession of the company, where it comes from, from whom, where and how this data is managed, making the various teams involved aware of it.

Once the DATA has been mapped, it is necessary to identify the gaps, so WHAT IS MISSING (GAP ANALYSIS) to fill these gaps and make the procedures adequate to the provisions of the GDPR and, we emphasize "adequate", remembering that the GDPR does not provide for the concept of "measures minimum" present instead in the current "privacy" legislation.

3.RISK ASSESSMENT

Once we have understood what is missing, it is necessary to define what they will bethe ACTIONS NECESSARY to adapt the current processing procedures and make them compliant by the date of application of 25 May 2018 as well as, what is needed to update and maintain them even after this deadline.

4.Create a ROADMAP

First of all, it is essential that all the Roles are clear and defined and everything goes in the right direction. In this phase, the DPO's supervisory and coordinating role is fundamental, not only to control and supervise but, also to provide advice and training to the resources involved and, above all, to monitor, with the help of "Audit" tools, which do not data breaches in which case, it will have to promptly intervene to manage the Data Breach with the Supervisory Authorities.

One of the most important innovations introduced and which, beyond the important penalties envisaged, leads more than any other to take the GDPR seriously, is precisely the Notification Obligation or Data Breach Notification.

The penalties provided for by European Regulation 2016/679 are not insignificant, so need consider this EU regulation.