New E.U. Regulation on the Protection of Personal Data ("General Data Protection Regulation - GDPR")

Introduction to the new rules and description of a possible methodological approach

The European Commission has been working since 2012 on developing a data-protection package whose purpose is to respond to the needs of citizens who are concerned about the risk of losing control over their own personal data because of the massive spread of technologies that enable the collection and handling of huge quantities of data regarding people's behaviour (e.g. via social network applications and the Internet of Things). The package contains two different tools: the Regulation and the Directive. In this introduction we shall focus on the **Regulation** concerning "the protection of natural persons with regard to the processing and free flow of their personal data". The Regulation aims to govern the processing of personal data in both the private sector and the public sector in all of the European Union's Member States. It was adopted by the European Parliament in April 2016 and will become **definitively and directly applicable in all EU countries as of May 25, 2018.** It defines the pecuniary administrative sanctions established to punish infringements of its provisions, up to a maximum fine of **€20 million or up to 4% of the offender's total worldwide sales in the prior year,** if higher. The following chart shows the areas now covered by the **Regulation,** as compared to the Italian legislation currently in force (Personal Data Protection Code):

1. **Accountability:** the GDPR promotes the **accountability** of the individuals and units responsible for the processing of personal data, and for the adoption of approaches and policies that constantly take account of the risk that a particular type of treatment of personal data might pose for the rights and freedoms of the individuals concerned.
2. **Data Protection Officer ("DPO"):** a new figure introduced by the **Regulation.** The DPO must be designated by the officer responsible for the processing, and must carry out his or her functions in full **independence** and in the **absence of any conflict of interest.**
3. **Information sheet:** the new Regulation establishes **clearer rules** for the information sheet and the consent form, and sets precise restrictions on automated data processing, on violation of the rules and on data exchange outside the European Union.
4. **Data Protection Impact Assessment (DPIA):**
   4.1 Each officer responsible for data processing is required to conduct and document a **self risk assessment** before

UHY Italy provides a wide variety of services, ranging from corporate and organizational consulting, to corporate assistance, as well as tax and consulting assistance, audit, payroll and outsourced services.

UHY Advisor Srl, UHY Associati Stprl, UHY Bompani Srl, FiderConsult Srl are all members of UHY Italy

Our partners are certified professionals with years of experience in public practice and with leading international firms.

Via Birmania 81
00144 Roma
Tel. +39 06 591.74.69
Fax +39 06 591.35.82

Via Bernardino Telesio 2
20145 Milano
Tel. +39 02 480.12.534
Fax +39 02 481.81.43

Viale Giuseppe Mazzini 26
50132 Firenze
Tel. +39 055 234.79.02
Fax +39 055 234.79.09

www.uhyitaly.com
info@uhyitaly.com

starting a type of processing that might present a high risk for *"individuals' rights and freedoms"*.

4.2 The officer responsible for data processing is required to consult the relevant supervisory authority **before performing the assessment** if its potential impact on data protection presents a high risk.

4.3 DPIA is an **essential** process for evaluating the necessity and proportionality of the countermeasures to be implemented in order to manage the risks entailed in treating personal data.

5. **Rights of the persons concerned:** the Regulation introduces new prerogatives recognized for the persons concerned by the processing, taking account of the present state in the development of new technologies. The Right to **erasure (**the so-called Right to be forgotten), the Right to **data portability** and the Right to **impose restrictions.**
6. **Privacy by design and by default:**
   6.1 The measures suitable to protect data must be implemented as soon as the need of processing arises and as of the creation of the means with which to do so (**privacy by design**).
   6.2 The processing must be performed solely for the purposes for which it was authorized and for the period of time strictly necessary for those purposes (**privacy by default).**
7. **Log of processing activities:** the Regulation introduces the obligation for the person responsible for the processing (the "controller" or "processor") to **keep a record** *"in electronic form or otherwise"* of the types of processing performed. This log must contain certain specific details, such as, for example, the purposes of the processing, a description of the categories of persons concerned, a general description of the technical and organizational security measures implemented, etc.
8. **Notification of a data breach:** the Regulation also introduces the obligation for the controller or processor to **notify** the relevant supervisory authority of any infringement of the personal data processing rules, and to do so without unjustified delay, if feasible **no more than 72 hours** after learning that such an infringement has occurred.

To comply effectively with the rules established by the GDPR, **each company must prepare a compliance plan of its own,** one that meets its own needs and takes account of the real impacts of the rules, giving priority to the principle of proportionality. Organizations that differ in size and in complexity must reconcile as far a possible the need to comply with the economic and organizational sustainability of the new privacy legislation.

The new Regulation has a transversal impact throughout a company's organization, **and requires multidisciplinary working groups** to respond adequately to the new rules. The following corporate functions or management units will be involved: Human Resources, Organization, Legal Affairs, Compliance, Information Systems, as well as the individual officers responsible for data processing.

UHY Italy, a member of the **UHY International** network of business consulting and auditing firms**,** suggests to its clients a four-fold approach to achieving compliance with the European Privacy Regulation:

1. **Analysis and evaluation of the AS-IS:** evaluation of the organizational model currently used to manage and privacy matters and of the technical and organizational control measures already in place.
2. **Gap analysis and definition of a compliance roadmap:** based on the results of the AS-IS analysis and evaluation, the next step will be to evaluate the necessary organizational changes and to perform a gap analysis with the aid of an appropriate tool. At the end of this phase, a compliance roadmap will be prepared.
3. **Definition of the methodology to be used in performing the DPIA** (Data protection Impact Assessment) and the protection profiles to be applied in the various ways of processing personal data;
4. **Implementation of the compliance plan:** the next step is to identify the ways in which the company's data processing systems need to be improved,

and to define and document the Data Protection Officer's tasks. Our firm provides support for the client's information systems in evaluating the technical and organizational measures already implemented, in order to ensure their adequacy in respect of the protection profiles that have been identified.

September 20, 2017

♣ ♣ ♣

Visit our web:
http://www.uhyitaly.com.

For further information:
info@uhyitaly.com