The new European privacy regulation comes into effect in May 2018

Maurizio Iorio, Attorney at Law

The new Regulation No. 679/2016, also known as The General Data Protection Regulation (GDPR), will enter into force in all EU countries on 25/05/2018, replacing almost entirely from this date the previous Italian Legislative Decree 196/2003 (Personal Data Protection Code).
In this issue of Market Place, I will briefly and succinctly examine the main features and some major innovations of the new Regulation, with a special focus on the 'novelties' that businesses will have to face. Given that this is a complex subject, I apologize in advance for the lists of information, cases/sub-cases and details, which I nevertheless tried to reduce to the minimum.

Scope of the Regulation

The GDPR applies to all processing[1] of personal data[2]: (1) relating to natural persons and (2) contained in a filing system or destined to converge into it, regardless of whether the processing is automated or not.
The scope of the GDPR excludes: **(1)** data processed by natural persons for personal or household purposes (e.g. phone book or email list for personal use), **(2)** data processed by public authorities, **(3)** data that do not fall within the scope of EU law.
Specifically, the GDPR applies only to the processing of personal data carried out by:
(1) data controllers or processors established in the EU, or
(2) data controllers or processors not established in the EU who offer goods or services to data subjects in the EU or monitor the behaviour of data subjects in the EU, or
(3) data controllers established in a non-EU country subject to the law of a EU country.
Examples of data ordinarily processed by a commercial company: data relating to personnel (recruitment, remuneration, management, administration); data relating to suppliers of goods or services if natural persons (thus including professional providers); data relating to customers or other physical third parties (e.g. journalists).
New: **(1)** Under the previous Legislative Decree 196/2003, also the processing of data not contained/converging in a filing system was covered by its provisions; **(2)** The GDPR identifies 'special categories of personal data' requiring consent and specific precautions for its processing; such data includes genetic data, biometric data, data concerning health, data which reveal racial or ethnic origin, party or trade-union membership, religious or philosophical beliefs (the underlined data is a novelty with respect to Legislative Decree 196/2003, which generally referred to it as 'sensitive data').

Overview of the content of the GDPR

The mechanism for the acquisition and processing of data is established by the GDPR combined with the rules for the protection of the rights and freedoms of the data subjects. It is basically divided into the following activities that will be summarized and examined below:

1- **Provision of information** to the data subject;
2- **Informed consent** from the data subject;
3- **Data processing methods** which must be complied with by law;
4- **Rights** granted to the data subjects.

[1] **Processing**: Any operation (automated or not) performed upon personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Please note that the underlined parts are new inclusions or rewordings with respect to the previous Legislative Decree 196/2003.

[2] **Personal data**: Any information relating to an identified or identifiable natural person ('data subject') by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. Please note that the underlined parts are new inclusions or rewordings with respect to the previous Legislative Decree 196/2003. Overall, the definition of 'personal data' is broader and more structured than the previous one.

1 PROVISION OF INFORMATION to the data subject

- There is the requirement of **enhanced information** as additional information must be provided to the data subject compared to Legislative Decree 196/2003. The list of information to be provided – which varies depending on whether personal data are collected from the data subject or not – is set out in Articles 13 and 14 of the GDPR and is awesome in terms of meticulousness and scope.

- Information must be provided **in writing** or even **electronically**, but, at the request of the data subject (provided his identity is proven in writing or by other means), it can also be **oral**.- Information may also be provided with **standardised icons** in order to give an overview of the intended processing.

2 INFORMED CONSENT from the data subject (indispensable prerequisite)

- The consent must be **free, specific, informed**, and **"*should be given by a clear affirmative act*"** (which excludes, for example, the use of pre-ticked boxes on forms) but does not necessarily have to be written or expressed in writing.

- **No consent is required: (a)** if the personal data processed does not allow to identify even indirectly the data subject; **(b)** when it does not involve 'certain' data and there is the need to enforce a contract or contractual provisions; **(c)** when it does not involve 'certain' data and there is a legal processing obligation; **(d)** when there is the need to protect the vital interests of the data subject or others; **(e)** for the execution of public interest tasks involving the exercise of public authority; **(f)** when it does not involve 'certain' data and the legitimate interest of the controller balances that of the individual to whom the data relates (e.g. customers data, employees data – including intra-company data transmission, physical safety, debt recovery even out of court, marketing research under certain conditions, etc.).

- **Consent is instead required: a)** save for specific exceptions, for 'certain' data (whose processing is permitted only subject to certain conditions), i.e. data relating to racial and ethnic origin, party or trade-union membership, religious or philosophical beliefs, health status or sexual orientation, genetic/biometric data; **b)** for data subject profiling purposes; **c)** for transferring the data subject's personal data to a non-EU country or an international organization.- **Consents obtained before** the GDPR came into force (thus under Legislative Decree 196/2003) are still valid and do not need to be renewed, provided the broad principles laid down in the GDPR are followed.

- It is expressly forbidden to condition the execution **of a contract or the provision of a service** on the consent to the processing of data NOT necessary for this purpose.- Consent **can always be withdrawn**.

- The collection and processing of data **without the data subject's consent carries heavy fines**.

3 DATA PROCESSING METHODS

- The **previous processing notification requirement** has been eliminated and replaced by a prior '**Data protection impact assessment**' (https://protezionedatipersonali.it/valutazione-impatto-e-rischio-trattamento) and by a '**Record of processing activities**' (https://protezionedatipersonali.it/registro-dei-trattamenti) which must be maintained, including in electronic form, by both the controller and processor: such requirement applies to enterprises with more than 250 employees while for the others (probably most of them) it is required if the processing carried out (i) is likely to have risk profiles and (ii) the processing is not occasional or includes 'certain' personal data.

- One of the main principles imposed by the GDPR is the **obligation of accountability**, i.e. a filing system for the management of data confidentiality which must be accurate and regularly updated.

- **Parties responsible for data processing:**

DATA CONTROLLER is the natural person or entity that is in control of the processing of personal data; he must implement appropriate technical and organizational measures in order to achieve compliance of data processing in accordance with the GDPR and provide evidence thereof (e.g. adoption of specific codes of conduct or company certifications);

DATA PROCESSOR is the natural person or entity that processes personal data on documented instructions from the controller through a "*contract or other legal act*", although chains with intermediate rings are possible (e.g. controller, processor/sub-processor).

PARTIES AUTHORISED TO PROCESS DATA: the controller is required to expressly indicate the persons authorised to process personal data in the enterprise to which he belongs (and thus, for example, human resources personnel processing personal data including the health data of employees, or in charge of producing the payslips showing the contributions to trade union organisations).

DATA PROTECTION OFFICER (DPO): top-level figure (very different from the data processor); the appointment of the DPO is mandatory only in case of processing that by nature or purpose require a large-scale, regular and systematic monitoring of the data subjects; the DPO must be able to operate (also in terms of spending capacity) in an autonomous and independent manner, outside the control or sanctioning power of the data controller or processor; he must have specific expertise which must be kept constantly up to date; he may – notwithstanding the above – be an employee of the controller or processor, or an external consultant who performs this task on the basis of a service contract.

4 RIGHTS GRANTED TO THE DATA SUBJECTS

- **Transparency**: personal data must be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*". (Art. 5.1 (a) of the GDPR).
- **Provision of information**: we have already talked about it in this article.
- **Access to personal data**: the right to obtain a copy of the data processed; to obtain an indication of the conservation period; to know the data protection policy in the event of transfer to third countries.
- **Rectification**: the right of rectification, already provided for under Legislative Decree 196/2003, is explicitly stated in Art. 16 of the GDPR: it consists of the right to obtain the rectification, correction or updating of personal data and (new) the right to have **incomplete personal data completed**.
- **Objection to the processing**: in some specific cases the data subject can now object to the processing of personal data without providing any reasons, while in other cases he can only object by putting forward specific reasons.
- **Right to be forgotten**: right previously not explicitly provided for: the data subject has the right to obtain the erasure of personal data (e.g. request to de-index a web page in search engines or to erase information from a website).
- **Restriction of processing**: right, now provided for by the GDPR, not only in the case **of violation** of the conditions of lawfulness attached to processing (as an alternative to the erasure of data), but also if the data subject requests the **rectification** of data and, pending such rectification, **objects** to its processing.
- **Data portability**: right previously not explicitly provided for: the data subject has the right to receive the personal data which he has provided to an online company and transmit it to other web operators or request, if technically possible, its transmission from one controller to another.
- **Profiling**: right previously not provided for: the data subject has the right not to have his personal data subjected to automated processing aimed at evaluating certain personal aspects and/or categories of interests without human intervention.
- **Protection based on one-stop-shop**: right previously not explicitly provided for: the data subject has the right to report any violations regarding himself to a competent local supervisory authority (the 'Guarantor for the protection of personal data' in Italy) placed under the coordination of an EU entity (European Control Committee, successor to the current 'Article 29 Working Party': http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358).

For further information: http://www.garanteprivacy.it/web/guest/home_en

4

Maurizio Iorio, Attorney at Law

_____