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

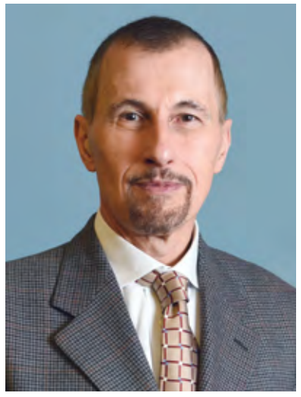
Maurizio Iorio, Attorney at Law

_____

di Maurizio Iorio

GDPR: IN VIGORE A MAGGIO IL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

Il nuovo regolamento N. 679/2016 (noto anche come GDPR, acronimo di General Data Protection) entrerà in vigore in tutti i paesi UE il 25.05.2018, sostituendo, in Italia, il precedente D. Lgs 196/2003 (Codice in materia di protezione dei dati personali). In questo numero di MarketPlace esaminiamo le principali caratteristiche del Regolamento e alcune innovazioni, con un occhio particolare alle "novità" per le imprese. Trattandosi di materia complessa, chiedo in anticipo scusa per gli elenchi di informazioni, di casi, sotto casi e di dettagli, che ho comunque cercato di ridurre al minino.



MAURIZIO IORIO

Dalla partnership tra Marketplace e ANDEC prende vita questa rubrica, curata dall'Avvocato Maurizio Iorio, nel suo duplice ruolo di Avvocato Professionista in Milano e di Presidente di ANDEC.

Ambito di applicabilità:

Tutti i trattamenti[1] dei dati personali[2]: (1) relativi a persone fisiche e (2) contenuti in un archivio o destinati a confluirvi. Ciò indipendentemente dal fatto che il trattamento sia automatizzato o meno.

Sono esclusi i dati trattati **(1)** da persone fisiche per attività personale o domestica (ad es. rubrica telefonica o e-mail ad uso personale), **(2)** quelli trattati da autorità di pubblica sicurezza, **(3)** quelli che non rientrano nell'ambito di applicazione del diritto UE.

In particolare, ricadono nel GDPR solo i trattamenti effettuati da:

(1) titolare o responsabile stabilito nella UE oppure,

(2) titolare o responsabile non stabilito nella UE ma : a) relativi ad interessati che si trovano nella UE e concernenti b) l' offerta ai medesimi di beni o servizi anche gratuiti o il monitoraggio del loro comportamento in ambito UE oppure,

(3) titolare stabilito in stato extra UE soggetto al diritto di uno stato UE.

Esempi dati comunemente "trattati" da una società commerciale, dati relativi al personale (assunzione, retribuzione, gestione, amministrazione); dati relativi a fornitori di beni o servizi (inclusi quindi i professionisti) se persone fisiche; dati relativi a clienti o ad altri terzi persone fisiche (ad es. giornalisti).

Novità: **(1)** Sotto il precedente Dlgs 196/2003 anche i trattamenti di dati non contenuti / confluenti in un archivio erano coperti; **(2)** Il Regolamento identifica "Categorie particolari di dati personali, che per il trattamento richiedono il consenso e particolari cautele; si tratta di: dati relativi alla salute; dati genetici; dati biometrici, dati che rivelino l'origine razziale o etnica, le opinioni politiche o sindacali, le convinzioni religiose o filosofiche (le parti sottolineate costituiscono novità rispetto al Dlgs 196/2003, in cui si parlava invece genericamente di "dati sensibili").

Contenuto del Regolamento

Il meccanismo di acquisizione ed elaborazione dei dati viene dal Regolamento coniugato con la salvaguardia dei diritti delle persone fisiche interessate. Esso si articola sostanzialmente nelle seguenti attività, che saranno riassunte ed esaminate qui di seguito:

1- **Informativa all' interessato** circa il trattamento dei dati personali;

2- **Acquisizione del consenso dell'interessato** al trattamento dei suoi dati.

3- **Modalità di trattamento** che devono essere rispettate per legge.

4- **Diritti** riconosciuti agli interessati.

1- Trattamento: qualsiasi operazione automatizzata o meno applicata a dati personali come la raccolta, la registrazione, l' organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l' interconnessione, la limitazione, la cancellazione o la distruzione. Nota: le parti sottolineate costituiscono novità o riformulazioni rispetto al precedente Dlgs 196/2003.

2- Dato personale: qualsiasi informazione concernente una persona fisica identificata o identificabile (interessato) tramite un qualsiasi riferimento quale nome, numero di identificazione, dati relativi all' ubicazione, identificativo on-line o tramite uno o più elementi che caratterizzino la sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale . Nota: le parti sottolineate costituiscono novità o riformulazioni rispetto al precedente Dlgs 196/2003. Nel complesso la definizione di "dato personale" è più vasta e articolata di quella precedente .

1 - INFORMATIVA all' interessato circa il trattamento dei dati

- Si parla di **informativa "rafforzata"** in quanto all'interessato vanno fornite informazioni aggiuntive rispetto a quelle del Dlgs 196/2003: l' elenco delle informazioni da fornire – che varia a seconda che i dati siano raccolti o meno presso l' interessato - è riportato agli artt. 13 e 14 del Regolamento ed è "impressionante" per la sua minuziosità e portata;
- l' informativa va resa **per iscritto** o anche **telematicamente**; tuttavia, su richiesta dell'interessato (purché l' identità di questo sia comprovata per iscritto o con altri mezzi), l'informativa può essere anche **orale;**
- le informazioni possono essere date anche con **icone standardizzate** in grado di fornire un quadro d'insieme

2 - CONSENSO dell'interessato al trattamento dei dati (prerequisito indispensabile)

- Il consenso deve essere **libero, specifico, informato, manifestato *"attraverso dichiarazione o azione positiva inequivocabile"*** (quindi no, ad esempio, a caselle pre-spuntate su un modulo) ma non deve essere necessariamente scritto né manifestato per iscritto .
- **Non occorre il consenso**, **(a)** se i dati personali trattati non consentono neppure indirettamente di identificare, **(b)** quando non si tratti di dati "particolari" e c'è necessità di esecuzione di un contratto o misure contrattuali; **(c)** quando non si tratti di dati "particolari" e sussiste un obbligo legale al trattamento dei dati; **(d)** quando sussista una necessità di salvaguardia di interessi vitali dell'interessato o di altri; **(e)** per l'esercizio di compiti di interesse pubblico connesso all'esercizio di poteri pubblici; **(f)** quando non si tratti di dati "particolari" e il "legittimo" interesse del Titolare del trattamento bilancia quello del soggetto a cui i dati si riferiscono (ad es. dati di clienti, a dipendenti - inclusa trasmissione di dati in ambito intra-societario - sicurezza fisica, recupero crediti anche stragiudiziale, ricerche di marketing a certe condizioni ecc.).
- **Occorre invece il consenso: a)** salvo specifiche eccezioni, per i dati "*particolari*" (il cui trattamento peraltro è lecito solo ricorrendo alcune circostanze) ossia per i dati relativi a: origine razziale ed etnica, opinioni politiche o sindacali, convinzioni religiose o filosofiche, salute e vita sessuale, dati genetici, biometrici; **b)** per la profilazione dell'interessato ; **c)** per trasferire i dati dell' interessato presso un paese extra UE o in un'organizzazione internazionale.
- Il **consenso raccolto prima** dell'entrata in vigore del Regolamento (quindi sotto la L. 96/2003) è ancora valido e non necessita di esser rinnovato, purché siano rispettati i principi di massima di cui al Regolamento (ovvero, necessità di check aziendale)
- È espressamente vietato subordinare l'esecuzione **di un contratto o la prestazione di un servizio** alla prestazione del consenso al trattamento di dati che NON son necessari a tal fine
- Il consenso **può sempre essere revocato**.
- La raccolta e il trattamento di dati **senza consenso dell'interessato** è severamente sanzionata .

3 - MODALITA' DI TRATTAMENTO

- **È eliminato il previgente obbligo di notifica** preventiva dei trattamenti, sostituito da (a) una preventiva "**Valutazione di impatto**" (http://bit.ly/2u1Szki) e dalla registrazione in un apposito **"Registro delle attività di trattamento"** (http://bit.ly/2FLJIJ1) da redigersi anche in formato elettronico sia dal Titolare sia dal Responsabile del trattamento: il registro è sempre obbligatorio per le imprese sopra i n. 250 dipendenti , mentre per le altre (probabilmente la maggior parte delle aziende) lo è se il trattamento svolto (i) presenta profili anche normali di rischio e (ii) non è occasionale o include dati personali "particolari".
- È previsto ***l' obbligo di "accountability"*** ossia di un sistema documentale di gestione della riservatezza dei dati, che devono esser esatti e regolarmente aggiornati.
- **Soggetti PRIVACY aziendale :**

TITOLARE: è colui che decide le sorti del trattamento; egli deve attuare misure tecniche ed organizzative ade-

guate al fine di realizzare la conformità dei trattamenti di dati secondo il Regolamento e fornirne prova (utilità di adesione a codici di condotta o certificazioni aziendali specifiche);
RESPONSABILE : è colui che opera per conto del Titolare in modo documentato tramite "c*ontratto o altro atto giuridico* "; sono possibili catene con più anelli intermedi (ad es. Titolare, Responsabile, Sub Responsabile).
PERSONE AUTORIZZATE AL TRATTAMENTO (= gli ex "incaricati"): il Titolare ha l'obbligo di indicare espressamente le persone autorizzate al trattamento nella struttura che a se fa capo; da qui questa figura (ad es. impiegata dell'ufficio personale che tratta i dati, anche sanitari, dei dipendenti o addetta alla contabilizzazione dei cedolini paga riportanti la trattenuta di contributo al sindacato).
DATA PROTECTION OFFICER (o "Responsabile della Protezione dei dati"), acronimo DPO: figura apicale (ben diversa dal semplice " Responsabile del trattamento"); la nomina del DPO è obbligatoria solo nel caso di trattamenti che per natura o finalità richiedono un monitoraggio su larga scala, regolare e sistematico degli interessati; il DPO deve esser autonomo (anche sotto il profilo della capacità di spesa) e indipendente, sottratto al potere disciplinare o sanzionatorio del Titolare o del Responsabile; deve avere conoscenze specialistiche e tenerle aggiornate; egli può essere – fatto salvo quanto sopra - un dipendente del Titolare o del Responsabile oppure un consulente esterno che svolge tale funzione sulla base di un contratto di servizi.

4 - DIRITTI RICONOSCIUTI AGLI INTERESSATI
- **Trasparenza**: i dati personali sono "*trattati in modo lecito, corretto e* ***trasparente*** *nei confronti dell'interessato*".(art. 5.1, a del Regolamento).
- **Informativa**: se ne è già scritto nel presente articolo.
- **Accesso**: diritto a ottenere una copia dei dati trattati; a ottenere l'indicazione del periodo di conservazione; a conoscere la garanzia di protezione nel caso di trasferimento verso Paesi terzi.
- **Rettifica**: il diritto di rettifica, già previsto sotto il Dlgs 196/2003, è espressamente affermato all'art. 16 del Regolamento: esso consiste nel diritto di chiedere che i dati siano modificati, corretti o aggiornati e, (novità) che siano **integrati i dati personali incompleti**.
- **Opposizione al trattamento**: ora, in alcuni caio specifici l'interessato può opporsi al trattamento senza fornire alcuna motivazione, in altri può opporsi solo deducendo motivazioni specifiche.
- **Oblio**: diritto precedentemente non espressamente previsto: l' interessato ha diritto ad ottenere la cancellazione dei dati (es. richiesta di deindicizzazione di una pagina web nei motori di ricerca o di cancellare informazioni da un sito Web).
- **Limitazione del trattamento**: diritto previsto ora non solo per il caso **di violazione** dei presupposti di liceità del trattamento, in alternativa alla cancellazione dei dati, ma anche qualora l'interessato chieda la **rettifica** dei dati (in attesa di tale rettifica) o si **opponga** al loro trattamento.
- **Portabilità dei dati**: diritto precedentemente non espressamente previsto: l' interessato ha diritto di chiedere la restituzione di dati personali forniti a un'azienda che opera on-line e trasmetterli ad altri operatori del Web o di chiedere, se tecnicamente possibile, la trasmissione da un titolare all'altro.
- **Profilazione** : diritto precedentemente non previsto: l' interessato ha diritto a che i suoi dati personali non subiscano suddivisione automatizzata secondo categorie di interessi e/o caratteristiche, senza intervento umano.
-**Tutela tramite Sportello Unico**: diritto precedentemente non espressamente previsto: l' interessato ha diritto a rivolgersi ad un'autorità di sorveglianza locale preposta per raccogliere la segnalazione di violazioni che lo riguardano (in Italia il "Garante per la protezione dei dati personali") posta sotto il coordinamento di un'entità UE (Comitato di Controllo Europeo, erede dell' attuale "Gruppo Articolo 29" http://bit.ly/2FMRrGq).
Per approfondimenti: http://www.garanteprivacy.it/diritti-degli-interessati