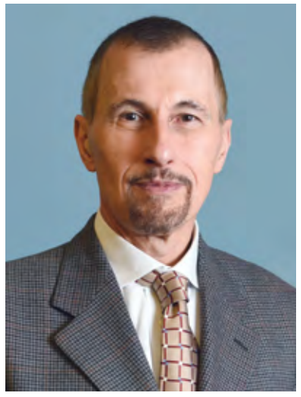
di Maurizio Iorio

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