Privacy e studi professionali

Avv. Monica Meroni

Seminario del 17 Maggio 2018

La normativa

- **Il Regolamento Europeo n.679/2016 (General Data Protection Regulation- GDPR) è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016**.
- Sarà applicabile in via diretta in tutti i Paesi UE dal **25 MAGGIO 2018**
- **Il Consiglio dei Ministri ha approvato, in data 10/05/2015, uno Schema di Decreto Legislativo (nuova bozza) per l'adeguamento della normativa nazionale alle disposizioni del Regolamento U.E, con conseguente abrogazione del Decreto Legislativo 30 giugno 2003 n.196, il c.d. Codice Privacy.**

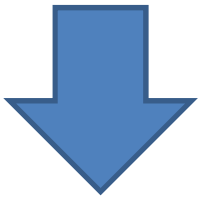
Il regolamento disciplina le modalità di

Trattamento dei dati personali delle

Persone fisiche

a) Sotto il profilo dell'informativa e consenso nella loro acquisizione

b) Sotto il profilo dell'utilizzo e circolazione dei dati



- Finalità:

Tutelare il diritto dell'individuo di disporre dei propri dati quali aspetti del fondamentale

Diritto di identità e di personalita'

ARTICOLO 8 C.E.D.U (Convenzione Europea dei Diritti dell'Uomo)

Diritto al rispetto della vita privata e familiare

1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*
2. *2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.*

Il principio sul quale si fonda il GDPR

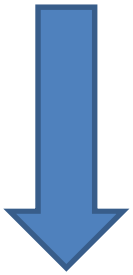
Principio di responsabilizzazione c.d.accountability – responsabilità del titolare del trattamento in merito al compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali

Natura non tassativa

delle indicazioni contenute del GDPR

ADEMPIMENTI PER I PROFESSIONISTI

Non sono « standardizzati» nel senso che il GDPR non continene un *elenco di adempimenti* da adottare da parte dei professionisti



Innanzitutto occorre partire dalla natura dei

I DATI TRATTATI

DATI PERSONALI: *«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*;

DATI SENSIBILI: *È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

- *Dati genetici;*
- *Dati biometrici;*
- *Dati relativi alla salute*

I dati raccolti devono essere:

1) Finalizzati: quindi pertinenti a quanto necessario per lo scopo del trattamento

2) Accurati: con verifica della loro correttezza e veridicità e completezza;

3) Limitati: quantitativamente a quanto necessario alle finalità dichiarate nell'informativa;

4) Utilizzati in modo riservato e confidenziale

Conservati ed archiviati non oltre il tempo necessario per la finalità del trattamento. Nel GDPR non viene indicato il periodo di tempo.

Dopo la raccolta dei dati, si passa alla fase del

Trattamento dei dati

Che cosa si intende per *trattamento?*

«qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di 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»

Come deve avvenire il TRATTAMENTO?

Il trattamento deve avvenire in modo:

a) **<u>Lecito</u>: si deve fondare sul CONSENSO dell'interessato;**

b) **<u>Corretto</u>: attraverso l'informazione dell'INTERESSATO circa la raccolta, utilizzo ed altri eventuali successivi trattamenti dei dati forniti;**

c) **<u>Trasparente</u>: con modalità predefinite e rese note all'interessato in modo chiaro, semplice ed accessibile.**

IL CONSENSO AL TRATTAMENTO DEI DATI

Prima di esprimere il consenso, l'interessato deve essere **compiutamente informato delle modalità e le finalità del trattamento dei dati.**

Come deve essere espresso il consenso?

In modo libero

In modo inequivoco;

In modo Specifico

Sono escluse forme di consenso tacito o mediante opzioni già selezionate.

Il Regolamento non prevede obbligatoriamente la forma scritta, anche se è la forma preferibile, poiché il titolare del trattamento deve essere in grado di dimostrare (in caso di violazione dei dati personali) che l'interessato ha prestato il proprio consenso.

Il consenso raccolto prima del 25 maggio 2018 resta valido se presenta tutti i requisiti indicati nel GDPR. In caso contrario è necessario raccogliere un nuovo consenso.

INFORMATIVA

Il Regolamento non prevede modelli predefiniti.

Il GDPR specifica le caratteristiche dell'informativa in modo più dettagliato rispetto al Codice della Privacy, il D. Lgs n.196/2003.

La forma dell' INFORMATIVA deve essere **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile.**

Occorre utilizzare un linguaggio chiaro e semplice.

***

Chi rilascia l'informativa?

IL TITOLARE DEL TRATTAMENTO che – di norma- nell'ambito del contratto tra professionista e cliente, coincide con la figura del professionista.

Quale sarà il contenuto dell'INFORMATIVA ?

Il contenuto dell'INFORMATIVA è elencato nell'articolo 13 e 14 del GDPR. Deve prevedere

- **I riferimenti di contatto del professionista (telefono; fax; posta elettronica certificata oppure ordinaria) per le comunicazioni relative all'esercizio del diritto;**
- **La descrizione precisa e dettagliata delle finalità per le quali viene posto in essere il trattamento;**
- **La specifica e chiara indicazione dei diritti di revoca del consenso, di accesso ai dati, di rettifica e di cancellazione (il c.d. diritto all'oblio) di limitazione del trattamento, di portabilità dei dati e di opposizione;**
- **Indicazione, ove esistente, dei dati di contatto del Responsabile della Protezione dati (R.P.D) o D.P.O;**

(segue il **Contenuto dell'informativa**):

- **Indicazione del periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione.**
- **Il diritto di presentare un reclamo all'Autorità di Controllo;**
- **Se il trattamento comporta processi decisionali automatizzati (anche la c.d. profilazione) l'informativa deve specificarlo, indicando la logica di tali processi decisionali e le conseguenze per l'interessato;**

****

Quando viene rilasciata l'INFORMATIVA?

L'informativa deve essere consegnata ai propri clienti, preferibilmente per iscritto. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta oppure dal momento della comunicazione dei dati.

REGISTRO DI ATTIVITA' DI TRATTAMENTO

L'obbligo di tenuta del registro delle attività di trattamento non è obbligatoria per il titolare del trattamento

che occupi meno di 250 dipendenti.

Obbligo prescinde dal requisito dimensionale nel caso in cui i dati oggetto del trattamento possono presentare rischi per i diritti e la libertà degli interessati oppure il trattamento non sia occasionale o includano dati sensibili, genetici, biometrici i o giudiziari cosi come individuati dall'articolo 9 e 10 del Regolamento.

Il 25 maggio 2018 è ormai alle porte…

Cosa deve fare ? Alcuni spunti di riflessione…

1. **Ho predisposto la modulistica per procedere, durante il primo incontro con il Cliente, alla raccolta dei dati fornendo al medesimo una informativa completa, con un linguaggio semplice e chiaro?**

2. Ho organizzato le mie attività in modo da raccogliere e trattare solo ed esclusivamente i dati che mi sono necessari o utili in vista del miglior espletamento dell'incarico ricevuto?

3. Ho organizzato la conservazione dei documenti relativi alle varie pratiche in modo da averne sempre, al momento giusto, la disponibilità ed in modo che i dati siano accessibili al solo personale autorizzato?

4. Ho nominato e adeguatamente istruito i miei collaboratori ed altresì ho formalizzato i rapporti con i professionisti ai quali mi rivolgo per la gestione e lo sviluppo delle attività dello studio?

5. I miei pc sono protetti dalle minacce esterne? Dispongo, in caso di bisogno, del nominativo di un tecnico-informatico di fiducia al quale chiedere la soluzione di specifici problemi?

6. P.C portatili e altri strumenti informatici rimovibili sono utilizzati, nelle attività al di fuori dello studio, in modo da minimizzare i rischi di perdita accidentale, sottrazione fraudolenta e similari?

7. Provvedo ad eseguire un salvataggio integrale (back up) di tutti i dati su pc?

8. Ho definito un tempo di conservazione dei dati personali in linea con le finalità dei trattamenti?

9. Quando devo rottamare pc, notebooks e altri strumenti elettronici utilizzati per le attività dello studio, mi assicuro che la dismissione avvenga nel rispetto della esigenza di protezione dei dati?

10. Mi sono preoccupato della sicurezza fisica dello studio, nel senso di adottare misure o cautele atte ragionevolmente a prevenire accessi indesiderati e azioni concretantesi nella lesione della riservatezza, della disponibilità, della integrità delle banche dati?

Le risposte costituiscono il punto
di « partenza» per gli adempimenti concreti
che ogni professionista deve adottare
nell’ambito della sua attività

Riassumendo, a titolo meramente esemplificativo, il professionista dovrà:

1) Riformulare la modulistica relativa alle informative, ai consensi, ai reclami , al diritto di accesso ai dati, privilegiando le modalità telematiche;
2) Rivedere e/o adottare misure per la sicurezza dei dati, in specie per il sistema informatico, con strategie di archiviazione, conservazione a norma e *disaster recovery;*
3) Adottare, ove previsto, il registro delle attività di trattamento, preferibilmente in forma elettronica;
4) Definire i ruoli del titolare del trattamento dei dati, ruoli e funzioni di eventuali « responsabili» per il trattamento dei dati e, opportuno, ma non obbligatorio, delegare specifiche funzioni agli « incaricati»;
5) Eventualmente, o necessariamente ricorrendone i presupposti, nominare un Responsabile della Protezione dei Dati o – in inglese- DPO – Data Protecion Officer;
6) Adottare Codici di condotta idonei, per esempio le certificazioni quando saranno disponibili e definite dalle relative Autorità;
7) Effettuare, sussistendone i presupposti, una Valutazione di impatto sulla protezione dei dati (assessment- art.35 GDPR).

Grazie per l’attenzione