



Brescia, li 8 maggio 2018

CIRCOLARE N. 3/18

A TUTTI I CLIENTI

LORO SEDI

**OGGETTO : Trattamento dei dati personali – Nuova disciplina europea riguardante la *privacy* (Regolamento UE 27.4.2016 n. 679)**

Il regolamento UE 27.4.2016 n. 679 ha sostituito la precedente disciplina in materia di *privacy* nel trattamento dei dati personali. Tale nuovo regolamento, che ha per oggetto la tutela delle persone fisiche nel trattamento dei dati personali e la libera circolazione di tali dati, sarà applicabile dal prossimo 25.05.2018.

Di seguito riportiamo le principali disposizioni che imprese, professionisti ed enti pubblici sono chiamati a rispettare a seguito dell'applicazione della nuova disciplina europea:

**1) Oggetto e ambito di applicazione**

Le nuove disposizioni si applicano :

a) a tutte le imprese, ai professionisti e alle pubbliche amministrazioni;

b) per la protezione delle persone fisiche con riferimento:

- al trattamento dei dati personali

- alla libera circolazione di tali dati;

c) con riferimento sia al trattamento di dati personali tenuto sia in forma automatizzata che in forma non automatizzata.

## 2) Figure previste dalla normativa

Oltre alle figure già previste dalla precedente normativa, ovvero il titolare del trattamento dei dati e il responsabile del trattamento dati è stata introdotta la nuova figura del responsabile per la protezione dei dati (DPO o RDP).

- a) Il titolare del trattamento è il soggetto, impresa individuale, professionista, società o ente che effettua il trattamento dei dati personali durante lo svolgimento dell'attività;
- b) Il responsabile del trattamento è il soggetto designato a trattare i dati personali per conto del titolare;
- c) **Il responsabile per la protezione dei dati (DPO o RDP)** è il soggetto, persona interna o esterna, dipendente o professionista, che è competente in materia di protezione dei dati personali. La nomina di tale nuova figura obbligatoria e deve essere comunicata per via telematica all'Autorità Garante privacy qualora :
  - il trattamento è svolto da un ente od organismo pubblico;
  - l'attività principale del titolare il trattamento dei dati richiede il monitoraggio regolare e sistematico di soggetti interessati su larga scala;
  - l'attività principale del titolare consiste nel trattamento dei dati come al punto precedente di categorie particolari di dati personali (condanne penali e reati);

La nomina può risultare obbligatoria anche in base al tipo di attività. Di seguito si riporta un elenco esemplificativo ma non esaustivo delle attività che potrebbero obbligare alla nomina della figura del responsabile per la protezione dei dati :

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici;
- sindacati nazionali;
- caf e patronati;
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

Tra i compiti svolti dal DPO (o RDP) si possono elencare i seguenti:

- informare e fornire consulenza al titolare e al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento dei dati;
- verificare l'osservanza del Regolamento;
- fornire pareri in merito alla Valutazione d'impatto sulla protezione dei dati ;
- tenere i contatti con l'Autorità Garante privacy e gli organi di controllo;

### **3) Adempimenti previsti dalla normativa**

Il titolare del trattamento, unitamente al responsabile del trattamento, dovrà predisporre la documentazione per poter effettuare tutti quegli adempimenti già previsti dalla precedente disciplina nonché quelli previsti da quella nuova :

- riguardo alle modalità di trattamento dei dati, all'acquisizione del Consenso al trattamento dei dati e al rilascio dell'Informativa;

- riguardo ai nuovi compiti ovvero tenere il Registro delle attività di trattamento ed alla redazione della Valutazione di impatto sulla protezione dei dati (DPIA);

### **4) Modalità di trattamento dei dati**

Il trattamento dei dati deve rispettare alcuni principi generali stabiliti dal Regolamento UE 27.04.2016 n.679 quali la liceità, la correttezza e la trasparenza nei confronti del soggetto interessato al trattamento, la limitazione delle finalità, la minimizzazione dei dati che devono essere adeguati, pertinenti e limitati e quant'altro necessario all'attività del titolare del trattamento al fine di garantire la riservatezza e l'integrità dei dati raccolti.

### **5) I rilascio del consenso al trattamento dei dati**

La nuova disciplina, contrariamente alla precedente, non precisa le modalità di acquisizione del consenso al trattamento che comunque deve essere libero, specifico rispetto alle finalità del trattamento e informato. Prevede il consenso esplicito solo per categorie particolari di dati sensibili . La richiesta di consenso qualora inserita all'interno di un formato deve essere distinguibile e resa comprensibile e facilmente accessibile con linguaggio semplice e chiaro.

### **6) L'informativa al soggetto interessato al trattamento dei dati**

L'informativa deve contenere un testo dettagliato dal linguaggio chiaro e semplice e facilmente accessibile scritto con una forma concisa, trasparente, intelligibile per l'interessato. Può essere resa oralmente, se richiesto dall'interessato, o per iscritto o con altri mezzi elettronici.

### **7) Principio di "responsabilizzazione" (*accountability*)**

La nuova normativa europea introduce il principio dell'*accountability* che consiste nella responsabilizzazione del titolare e dei responsabili del trattamento dei dati ora tenuti a mettere in atto tutte quelle misure tecniche e organizzative per garantire la riservatezza e la protezione dei dati nel procedimento del loro trattamento e per dimostrare la corretta applicazione della nuova normativa europea in materia di *privacy*

### **8) Diritti degli interessati al trattamento dei dati**

I diritti degli interessati al trattamento dei dati sono i seguenti :

- a) diritto all'accesso al trattamento dei dati ;
- b) diritto di rettifica al trattamento dei dati ;
- c) diritto di opposizione al trattamento dei dati ;
- d) diritto alla limitazione al trattamento dei dati, se non in contrasto con l'attività resa ;

e) diritto alla portabilità dei dati ovvero alla possibilità di trasferire i dati personali da un titolare del trattamento ad un altro indicato dall'interessato ;

f) diritto all'oblio (cancellazione) in forma rafforzata ovvero la possibilità di disporre al titolare del trattamento dei dati la cancellazione dei propri dati quando non siano più necessari rispetto alle finalità del trattamento o quando sia avvenuto il ritiro del consenso prestato o qualora si sia riscontrato il trattamento illecito dei dati.

## **9) Registro delle attività di trattamento**

Tra le novità introdotte dalla normativa europea sulla *privacy* c'è la tenuta di un registro delle operazioni di trattamento in formato cartaceo o anche elettronico. Sul registro dovranno essere annotate le misure di sicurezza tecniche ed organizzative adottate per la corretta gestione dei rischi derivanti dal trattamento dei dati. L'obbligo sussiste se il trattamento dei dati rappresenta un rischio per i diritti e le libertà dell'interessato, non è occasionale, include il trattamento di categorie particolari di dati giudiziari o di dati personali di tipo "sensibile" ovvero relativi alla salute, all'opinione politica, alle convinzioni religiose, alla vita sessuale, all'appartenenza sindacale, all'origine razziale o etnica della persona.

## **10) Valutazione di impatto sulla protezione dei dati trattati (DPIA)**

La nuova normativa europea ha introdotto altresì l'obbligo per il titolare del trattamento dei dati di effettuare una valutazione di impatto sulla protezione dei dati (DPIA) qualora il trattamento presenti un rischio elevato per i diritti e le libertà dell'interessato, vi siano trattamenti automatizzati anche con profilazione, trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali o a reati nonché trattamenti ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico.

## **11) Violazioni del trattamento dei dati**

La nuova normativa prevede che il titolare del trattamento notifichi ogni violazione dei dati trattati all'Autorità competente entro 72 ore dal momento in cui ne venga a conoscenza e, in casi gravi, anche all'interessato. L'obbligo sussiste soprattutto se si ritiene che tale violazione abbia gravi conseguenze per i diritti e le libertà di quest'ultimo

## **12) Controllo a distanza dei lavoratori (Videosorveglianza)**

Una particolare attenzione va prestata agli impianti di controllo a distanza dei lavoratori che devono rispettare le prescrizioni indicate dall'Autorità Garante privacy e dalla normativa in materia. La videosorveglianza è soggetta :

- al preventivo accordo con le Rappresentanze sindacali in caso di medie e grandi imprese;
- alla preventiva autorizzazione della Direzione Territoriale del Lavoro in caso di piccole imprese.

## **13) Adeguamento alla nuova normativa**

In sintesi si dovrà procedere, a comprova della conformità del trattamento dei dati alle nuove norme del Regolamento europeo sulla *privacy*, come di seguito :

- alla revisione nella gestione e organizzazione interna dell'impresa, del professionista o dell'ente pubblico, conformandola alla nuova normativa europea sulla *privacy*;
- alla contrattualizzazione dei rapporti tra il Titolare (e tra Titolari) e il Responsabile del trattamento dei dati, specificando le relative responsabilità;

- alla revisione della modulistica con l'interessato al trattamento dei dati, riformulando il documento dell'informativa e acquisendo il nuovo consenso al trattamento dei dati;
- alla programmazione e all'attuazione di sistemi atti a garantire la sicurezza e la protezione dei dati trattati;
- alla predisposizione della nomina del DPO (o RDP) , del Registro delle attività di trattamento dei dati, **ove obbligatori**, e , **soprattutto per le piccole attività**, alla predisposizione, del documento di Valutazione di impatto sulla protezione dei dati trattati(DPIA).

#### **14) Avvertenze per le piccole imprese e i piccoli studi professionali**

Per quanto riguarda in particolare i professionisti si consiglia di contattare i relativi Ordini professionali (soprattutto sanitari) i quali hanno già diramato da tempo le proprie istruzioni operative nonché la modulistica da approntare per far adeguare i propri iscritti alla nuova normativa europea.

Per le piccole imprese e per i piccoli studi professionali **è consigliata la predisposizione entro la scadenza del prossimo 25.05.2018** del documento di **Valutazione di impatto sulla protezione dei dati trattati (DPIA)** ,apponendo contestualmente **una marca da bollo da 2 euro al fine di dare un minimo di data certa al documento.**

#### **15) Fonti di informazione sulla nuova *privacy* europea**

Per un vostro maggiore approfondimento sono disponibili molte informazioni e modelli sul sito internet dell'Autorità Garante privacy [www.garanteprivacy.it](http://www.garanteprivacy.it) , tra cui anche il software gratuito di autovalutazione:<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268>

Lo studio rimane a vostra disposizione per eventuali ulteriori informazioni.

Cordiali saluti.

STUDIO POLI & ASSOCIATI