

Martelli Dott. Stefano

Tel. 055 3860077

Ordine Dottori commercialisti
ed esperti contabili

**A TUTTI I SIGNORI CLIENTI
LORO SEDI**

<i>CIRCOLARE N.4 DEL 24/05/2018</i>
--

GDPR - REGOLAMENTO 2016/679 ex PRIVACY

Faccio seguito alla precedente circolare per fermare la Vs. attenzione su queste disposizioni molto importanti per tutte le aziende.

Come Voi tutti sapete a decorrere dal 25 p.v. entrerà in vigore il nuovo regolamento sulla Privacy.

I cambiamenti principali derivanti da tale normativa riguardano la protezione dei dati personali che trattiamo nelle nostre aziende e il tipo di consenso che dobbiamo ottenere.

Difficile determinare i passi da fare in quanto dipendono da quali dati trattiamo e di come li trattiamo. Ad esempio in linea di massima i dati dei dipendenti, se usati esclusivamente ai fini di legge (elaborazione buste paga e relativi adempimenti) non necessitano di consenso, mentre se pubblicizziamo le loro foto sul nostro sito siamo obbligati ad ottenere un consenso esplicito all'azione.

I nuovi obblighi sono ripartiti tra diversi ruoli, principalmente Titolare (Data Controller) e Responsabile (Data Processor). Quest'ultimo è una figura che non è obbligatoria nel gran numero dei casi ma l'obbligatorietà (vedi art. 37) deve essere valutata caso per caso e deve essere persona con le dovute conoscenze (frequenza di corsi etc.).

Descrivere il trattamento, discernere quale ruolo ciascuna assuma in esso e, quindi, determinare le rispettive competenze, è il lavoro da fare. Da parte di ciascuna azienda.

Facciamo presente che è cambiato il "dato" da trattare: da "sensibile" diventa "personale" per cui ogni dato che sia atto a identificare una persona fisica (anche solo cognome e nome) deve essere **PROTETTO**.

Si consiglia di fare riferimento al sito del Garante dove troverete la normativa ed alcune delucidazioni sulla materia

Per un elenco delle "cose da fare" potrebbe utilmente essere fatto riferimento al garante privacy alla pagina web:

<http://www.garanteprivacy.it/web/guest/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali>

Di seguito indichiamo i principali punti da affrontare da subito:

1) Responsabile della protezione dei dati

Il Regolamento, in alcuni casi, prevede la designazione di un **responsabile della protezione dati (RPD)**, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer).

Anche questa è una conseguenza dell'approccio responsabilizzante che è proprio del Regolamento. Dovranno designare obbligatoriamente un RPD:

- le amministrazioni e gli enti pubblici, fatta eccezione per le autorità giudiziarie;
- tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il Regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Nel caso in cui venga nominato l'RPD è OBBLIGATORIA la comunicazione al garante.

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, deve:

- possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati.
- adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Attenzione

Non sono **richieste attestazioni formali** o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.

Attenzione

Il titolare o il responsabile del trattamento devono mettere a disposizione del responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Passando ai compiti attribuiti al Responsabile della protezione dei dati essi consistono sostanzialmente nel:

- sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);

- informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

2) Adempimenti

A fronte di alcune semplificazioni procedurali, vengono introdotti alcuni nuovi adempimenti.

Nella tabella che segue si riportano alcune delle principali novità.

<p>Registro dei trattamenti</p>	<p>Il registro dei trattamenti è obbligatorio per tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio.</p> <p>Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.</p> <p>Nel registro devono essere riportati:</p> <ul style="list-style-type: none"> il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, paragrafo 2 GDPR, la documentazione delle garanzie adeguate; ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative. <p>Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.</p> <p>Pur non essendo in molti casi obbligatori è consigliabile redigerne uno che potrà essere utile in caso di eventuali verifiche.</p>
--	--

Misure di sicurezza	<p>Le misure di sicurezza da adottare devono “garantire un livello di sicurezza adeguato al rischio” del trattamento.</p> <p>Il GDPR riporta una lista di tali misure (art. 32, paragrafo 1 GDPR) ma essa è da intendersi come una lista aperta e non esaustiva.</p> <p>Per lo stesso motivo, dopo il 25 maggio 2018, non ci saranno obblighi generalizzati di adozione di misure “minime” di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.</p> <p>È comunque possibile utilizzare specifici codici di condotta o schemi di certificazione per attestare l’adeguatezza delle misure di sicurezza adottate.</p> <p>Tuttavia, il Garante potrà definire linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti potranno restare in vigore le misure di sicurezza attualmente previste: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi.</p>
Notifica delle violazioni di dati personali	<p>A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all’Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque “senza ingiustificato ritardo”, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.</p> <p>Pertanto, la notifica (il cui contenuto è disciplinato dagli artt. 33 e 34 GDPR) non è obbligatoria, ma è subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.</p> <p>Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre “senza ingiustificato ritardo” (sono comunque previste alcune eccezioni indicate all’art. 34, paragrafo 3 GDPR).</p> <p>Si ricorda, inoltre, che è già disponibile un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico.</p>

Lo studio resta a disposizione per ulteriori chiarimenti fossero necessari, per quanto di nostra competenza.

li, 24 Maggio 2018

Cordiali saluti.

Dott. Stefano Martelli