



Le novità principali riguardano le regole sul trattamento dei dati personali, che non potrà essere limitato nel tempo ma funzionale al motivo per il quale sono stati raccolti. Ad aiutare sia le imprese, che i professionisti e consumatore nell'analisi di **cosa cambia** con l'entrata in vigore del **GDPR dal 25 maggio 2018** è il Garante per la protezione dei dati personali, con una guida ai punti più importanti della riforma UE:

Nuove informative e richieste di consenso al trattamento dei dati personali

Le attuali informative e le relative richieste di consenso predisposte per clienti, fornitori e dipendenti non saranno più conformi al nuovo dettato normativo e dovranno essere aggiornate; nuove informazioni dovranno infatti essere obbligatoriamente inserite nel testo quali, ad esempio, il periodo di conservazione dei dati o le modalità per proporre reclamo al Garante della Privacy.

Diritto all'oblio

È una delle novità di maggior impatto della nuova disciplina. Ogni cittadino potrà richiedere in qualsiasi momento (per giustificati motivi e sempre se tale richiesta non sia in contrasto con altre normative) al Titolare di cancellare completamente i dati personali che lo riguardano. Questo varrà anche per eventuali soggetti terzi coinvolti dal Titolare nel trattamento di tali dati (responsabili esterni). Sarà perciò necessario definire in maniera chiara una "filiera" di ogni singolo trattamento, in modo tale da comunicare a tutti i soggetti coinvolti il recepimento di tale obbligo. Quest'obbligo entrerà automaticamente in vigore allo scadere del periodo di conservazione dichiarato nell'informativa (vedi punto precedente).

Portabilità dei dati

Ogni cittadino avrà il diritto di far trasferire i propri dati, trattati elettronicamente, ad un altro titolare (ad esempio: cambiando il gestore del servizio di telefonia, il vecchio gestore dovrà trasferire tutti i dati del cliente al nuovo gestore) e il titolare dovrà adeguare i propri sistemi informativi in tal senso.

Nuove misure di sicurezza

Il trattamento dei dati personali effettuato mediante strumenti elettronici dovrà essere effettuato col rispetto di misure di sicurezza più complete ed efficaci rispetto a quelle attualmente in uso. Il nuovo Regolamento pone infatti ai titolari l'obbligo, tra gli altri, di "pseudonimizzare" i dati, di conferire ai propri sistemi caratteristiche di resilienza in grado di fronteggiare un incidente fisico o tecnico. Allo stesso tempo, però, viene meno l'obbligo di recepire delle misure "minime" di sicurezza che, invece, dovranno essere definite dallo stesso Titolare.

Registro dei trattamenti

Ogni titolare avrà l'obbligo di redigere e aggiornare almeno annualmente un registro di tutti i trattamenti effettuati. In pratica: un nuovo DPS. Tale obbligo, però, salvo casi particolari, sarà limitato alle organizzazioni con più di 250 dipendenti.

Comunicazione delle violazioni dei dati personali

In caso di violazione di dati personali da parte di soggetti terzi, sia essa avvenuta per incidente o per dolo, il titolare del trattamento dovrà notificare, entro 72 ore dal momento in cui ne è venuto a conoscenza, agli interessati e al Garante della Privacy, gli estremi di tale violazione. La mancata notificazione nei tempi e nelle modalità previste esporrà il titolare a gravi sanzioni.

Valutazione d'impatto sulla protezione dei dati

Per alcuni particolari trattamenti (al momento non è ancora stato precisato di quali trattamenti si tratti: sarà cura del Garante della Privacy, prima dell'entrata in vigore del Regolamento, definire l'elenco di tali trattamenti) il titolare dovrà redigere una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali contenente, oltre alla sintesi del trattamento, un'appropriata analisi del rischio e delle contromisure tecniche e organizzative adottate per contrastare tale rischio.

Nomina del Privacy Officer

Alcuni particolari categorie di titolari (al momento non esiste ancora una indicazione sufficientemente precisa di quali soggetti abbiano effettivamente tale onere; spetterà al Garante fare luce sul punto prima dell'entrata in vigore del Nuovo Regolamento) avranno l'obbligo di nominare un soggetto quale "Responsabile per la Protezione dei Dati Personali". Gli estremi identificativi del Responsabile dovranno essere comunicati al Garante della Privacy. Il Responsabile (o "Privacy Officer") avrà l'onere di garantire il rispetto del Regolamento all'interno della struttura organizzativa del Titolare.

Oltre a questi nuovi obblighi il Regolamento porta anche qualche semplificazione rispetto alla normativa vigente:

Notificazione

Per alcune tipologie di trattamenti (censiti all'art.37 del D.Lgs 196/03) vige oggi l'obbligo di notificare al Garante tali trattamenti. Tale obbligo, col nuovo Regolamento, viene totalmente abrogato.

Riscontro all'interessato

Oggi la normativa vigente pone in carico ai titolari l'onere di rispondere alle richieste di riscontro, da parte dell'interessato, entro il termine tassativo di 15 giorni (1 mese, in caso di comprovata difficoltà tecnica a dare seguito alle richieste dell'interessato). Tale termine, per effetto del nuovo Regolamento, è aumentato ad un mese (2 mesi in caso di comprovata difficoltà tecnica).

Età minima per la prestazione del consenso al trattamento

Attualmente la norma non consente ai minori di esprimere il consenso al trattamento dei propri dati personali: fino al compimento del 18° anno di età, infatti, solo un genitore o un tutore possono farlo, per conto del minore stesso. Con l'entrata in vigore del Regolamento UE, l'età minima per poter prestare legittimamente il consenso al trattamento invece, scende a 16 anni.

Contattaci per maggiori informazioni

Confcommercio Lecco / Piazza Garibaldi, 4 - Lecco
Tel. 0341.356911 - Fax 0341.284209 www.confcommerciolecco.it