



## **Entrata in vigore del nuovo regolamento Europeo Privacy 25 Maggio 2018**

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il Regolamento Europeo è entrato in vigore il 25 maggio 2016 e si applicherà in tutti gli Stati Membri a partire dal 25 maggio 2018, termine entro il quale le aziende dovranno adeguarsi alla nuova normativa.

Il Regolamento Europeo Privacy o GDPR introduce nuove tutele a favore degli interessati, e nuovi obblighi a carico di Titolari e Responsabili del trattamento di dati personali.

Con riferimento ai nuovi diritti riconosciuti all'interessato segnaliamo in particolare:

- **Diritto all'oblio:** può essere definito come il diritto di un individuo a non essere più ricordato per fatti che lo riguardano e che in passato sono stati oggetto di cronaca.
- **Diritto alla portabilità dei dati:** Il Regolamento prevede che quando i dati sono trattati con mezzi automatizzati l'interessato debba poter ricevere da un titolare del trattamento tutti i dati personali che lo riguardano in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile in modo da poterli all'occorrenza trasmettere ad un altro fornitore di servizi o comunque ad altro titolare del trattamento.

Per quanto concerne Titolari e Responsabili del trattamento riassumiamo di seguito gli adempimenti più rilevanti introdotti dalla normativa europea.

- **Il principio dell'accountability:** Il Regolamento pone l'accento sulla "responsabilizzazione" di titolari e responsabili – ossia, sull'adozione da parte dell'Azienda di comportamenti tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.
- **Registri delle attività di trattamento:** L'Azienda è tenuta a riportare tutte le attività di trattamento dati svolte sotto la responsabilità del titolare al trattamento o del responsabile in appositi registri. Il Garante non ha ancora. Il dovere di tenuta dei registri non si applica alle imprese o organizzazioni con meno di 250 dipendenti a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (nello specifico dati sensibili e biometrici o dati personali relativi a condanne penali e reati).
- **Il Privacy Impact Assessment (valutazione d'impatto sulla protezione dei dati).** E' una valutazione che l'Azienda deve operare prima del trattamento per soppesare la particolare probabilità e gravità del rischio per la protezione dei dati trattati. Mediante la valutazione d'impatto si acquisiscono le necessarie conoscenze sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio e assicurare la conformità del trattamento agli standard normativi. La valutazione d'impatto è richiesta per i trattamenti su larga scala e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato. Il Garante provvederà con apposito provvedimento a definire i casi in cui tale adempimento risulti necessario.



- Notifica del “data breach”: 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", se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati
- Designazione del Data Protection Officer (Responsabile della protezione dati). Il DPO è un professionista che possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, che sia in grado di adempiere alle proprie funzioni in piena indipendenza ed in assenza di conflitti di interesse e può essere tanto un soggetto interno all'organizzazione quanto un soggetto esterno. Il DPO dev'essere designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati e delle capacità di adempiere ai compiti. Il Titolare del trattamento deve mettere a disposizione del responsabile della protezione dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti. La designazione di un DPO sarà obbligatoria:
  - ✓ nel caso in cui il trattamento venga effettuato da un'autorità pubblica o da un organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali),
  - ✓ qualora le attività principali del Titolare e del Responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessi su larga scala,
  - ✓ nell'ipotesi in cui le attività principali di suddetti soggetti consistano in trattamenti su larga scala di categorie particolari di dati personali (dati sensibili, dati genetici, biometrici, dati giudiziari).

**per informazioni Ufficio Qualità Sicurezza Ambiente Energia Apindustria Brescia:**  
tel. 03023076 - fax 0302304108 - email [servizi@apindustria.bs.it](mailto:servizi@apindustria.bs.it)