

Nuovo Regolamento Privacy: Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016

Il 25 maggio 2018 entrerà in vigore il nuovo Regolamento Europeo in materia di protezione dei dati personali che prevede un nuovo modo di considerare la privacy e un diverso regime sanzionatorio per le imprese. La norma UE sarà applicabile immediatamente e sarà direttamente vincolante in ogni sua parte senza la necessità di alcun recepimento da parte della normativa interna per la sua efficacia.

La nuova normativa privacy risulta più flessibile, prevede meno adempimenti formali e più tutele per l'individuo. L'impostazione normativa del Regolamento è in effetti diversa da quella del precedente Codice della Privacy, gli adempimenti non sono descritti nella loro specificità di attuazione ma se ne indica la finalità, lasciando al titolare del Trattamento il compito di concretizzare quanto previsto. Un approccio di questo tipo aiuta gli operatori a maturare la consapevolezza che la protezione dei dati non è una questione puramente formale ma riguarda la sostanza stessa di svolgimento dell'attività imprenditoriale e per tale motivo diventa sempre più un aspetto imprescindibile e caratterizzante della stessa metodologia lavorativa.

Ecco i sei requisiti necessari per gestire in modo consapevole la Privacy, rispettando la nuova normativa Europea.

- **CONTESTO DI APPLICAZIONE:** artt. 2,3,6,24,25,32,35. Chiunque ha un'attività e gestisce i dati altrui è coinvolto, rimangono esclusi solo i soggetti privati nell'ambito della loro sfera personale. Diventa indispensabile formalizzare in un Documento di valutazione la situazione concreta dell'attività e i dati da essa gestiti. Questa fotografia analitica e costantemente aggiornata della realtà aziendale, rappresenta il presupposto su cui verranno costruite e implementate le successive misure di gestione del dato a tutela della privacy.
- **RUOLI E RESPONSABILITÀ SOGGETTIVE:** artt. 26-29. La norma identifica il titolare del trattamento (soggetto che ha in capo la responsabilità di gestire un dato altrui), i soggetti autorizzati al trattamento (i soggetti incaricati dal titolare che lavorano o utilizzano i dati nell'espletamento della propria attività) e i responsabili esterni (tutte quelle figure professionali, esterne all'impresa, che su incarico del titolare, hanno accesso ai dati, es: tecnico hardware, gestore del sito web, tecnico che verifica i filmati della telecamera esterna, ecc...).
- **MAPPATURA:** artt. 30-32 - fa riferimento al concetto di responsabilizzazione del titolare del trattamento, introdotto dal nuovo Regolamento Europeo. Si tratta di un lavoro di analisi della propria attività che evidenzia quale è il sistema di sicurezza adottato per i rischi specifici evidenziati. Si parte dalla mappatura dei dati gestiti, si passa all'analisi dei rischi possibili e infine si definiscono le azioni intraprese o da intraprendere tramite un'opportuna calendarizzazione degli interventi, per tutelare i dati. Il Regolamento non fornisce delle regole predefinite ma specifica le finalità della norma lasciando a ciascun Titolare di applicare al meglio, secondo la propria specificità, il dettato normativo.
- **GESTIONE DEGLI INCIDENTI:** artt. 33-34 - Questa parte incentiva la consapevolezza che ogni titolare deve acquisire in merito alla gestione degli incidenti sui dati. Ad esempio: cosa accade se i dati vengono danneggiati da un virus, tipo

criptoloker? o ancora, se si smarrisce la valigia o il portatile con dentro i documenti? La norma prevede in questi casi che il titolare predisponga delle procedure ben definite tramite le quali si proceda alla registrazione dell'evento e alla sua valutazione, per una sua adeguata gestione. Nei casi più gravi è prevista la denuncia al Garante entro le 72 ore successive all'evento.

- **INFORMATIVA:** artt. 12-14 - si tratta dell'informazione da rendere a tutti i soggetti a cui i dati appartengono. In questa fase è importante valutare a chi fornire l'informativa e che tipo di informativa produrre. Il documento in questione non può essere la semplice riproposizione del solito fac-simile da far sottoscrivere a chiunque indistintamente, in modo meramente burocratico e senza la minima consapevolezza del suo contenuto, ma è frutto di un'approfondita analisi risultante dalla gestione dei punti precedenti e di un'acquisita consapevolezza sia da parte del Titolare del trattamento che del proprietario dei dati. Alcuni esempi di differenziazione dell'informativa possono essere: comunicazione al dipendente, comunicazione al visitatore del sito web, informativa affissa sotto la telecamera, ecc... Le informative non devono essere generiche, ma specifiche alla realtà concreta a cui si riferiscono.
- **DIRITTI DELL'INTERESSATO:** artt. 15-22 - il titolare deve essere consapevole che il possessore dei dati ha dei diritti ben specifici, per questo motivo eventuali richieste ricevute in merito ai dati gestiti sono lecite e implicano l'obbligo di una azione positiva e ben specifica. Le linee guida previste dal Garante analizzano proprio questi casi e il Titolare deve attuarle pedissequamente, con i moduli appropriati e le dovute verifiche, onde evitare di commettere violazioni della privacy proprio nel cercare di adempiere ad uno specifico obbligo. In questi casi bisogna valutare la complessità delle richieste e prevedere tempi di risposta adeguati.

Ma cosa vuol dire fornire al dipendente una **informativa** chiara ed esaustiva sui dati raccolti. Il Garante già nel 2015 individuava in modo esemplificativo le regole per il corretto trattamento dei dati personali dei lavoratori da parte dei soggetti pubblici e privati:

- Il datore di lavoro può trattare informazioni personali solo se strettamente indispensabili all'esecuzione del rapporto di lavoro.
- I dati possono essere trattati solo dal personale incaricato assicurando idonee misure di sicurezza per proteggerli da intrusioni o divulgazioni illecite.
- Sul luogo di lavoro va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità delle persone garantendo la sfera della riservatezza nelle relazioni personali e professionali
- I trattamenti di dati personali devono rispettare il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di informazioni personali e identificative
- Si deve rispettare il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori
- I trattamenti devono essere effettuati per finalità determinate, esplicite e legittime in base ai principi di pertinenza e non eccedenza
- Il trattamento di dati personali, anche sensibili, è lecito, se finalizzato ad assolvere obblighi derivanti dalla legge, dal regolamento o dal contratto individuale.

La gestione dei dati relativi al rapporto di lavoro necessita di una particolare attenzione da parte del Professionista sia relativamente ai tipici dati legati ai cedolini paga ma soprattutto con riferimento a quelle informazioni legate al rapporto di lavoro che rientrano in una sfera

più intima e privata del dipendente; pensiamo ad eventuali trattenute sindacali, ai dati legati a un infortunio o a tutte quelle informazioni collegate al sempre più diffuso welfare aziendale. Proprio in questo ultimo caso la commistione di informazioni tipicamente personali necessarie alla predisposizione dei piani di welfare con i normali dati lavorativi, è sempre più frequente. La Raccomandazione adottata il 01 aprile 2015 dal Consiglio D'Europa ha previsto che la gestione dei dati relativi alla navigazione internet, l'accesso allo scambio delle comunicazioni digitali, l'elaborazione delle coordinate di geolocalizzazione possono essere considerate come trattamento dei dati personali del dipendente. Queste casistiche, sempre più diffuse, generano l'esigenza in capo all'azienda e ai suoi professionisti di una maggiore attenzione e tutela specifica, sia relativamente alla informativa e al consenso, che alla gestione complessiva del dato, secondo le varie sfaccettature previste dalla norma. Il Regolamento prevede in questi casi che le aziende forniscano un'INFORMATIVA preventiva al lavoratore. Tale informativa deve essere " trasparente, pertinente, proporzionale e non eccedente rispetto al trattamento". Rispetto al passato le informative dovranno essere più semplici e più efficaci, richiederanno quindi una maggiore **consapevolezza** da parte dell'azienda nella fase di predisposizione e una maggiore **consapevolezza** da parte del lavoratore durante la fase di recepimento e sottoscrizione. L'informativa si dovrà integrare con le previsioni specifiche previste dai Contratti Collettivi e con i codici di condotta interni eventualmente predisposti dall'azienda per l'utilizzo degli strumenti e l'effettuazione dei controlli. La Guida predisposta dal Garante analizza il caso specifico della gestione dei dati privati legati al rapporto di lavoro a pag 180 Par 8.2.

Luca Campagnoli
ODCEC Piacenza