Nuova Disciplina della Privacy

Vademecum per le micro e piccole imprese

- **COSA E'?**

Il 25 maggio 2018 entra in vigore il nuovo Regolamento Privacy.
Rappresenta un cambiamento di prospettiva e si applica a tutte le aziende, piccole e grandi, nel pubblico e nel privato.

Vi è un nuovo approccio che privilegia l'aspetto sostanziale (non più adempimenti meramente formali). L'azienda è **"responsabilizzata"** ad analizzare la propria situazione e gli eventuali specifici rischi prima porre in essere azioni concrete anche da un punto di vista organizzativo.

Non ci sono più le "misure minime" previste dall'attuale Codice della Privacy ma spetta al titolare del trattamento valutare se e come trattare i dati, quali sono i rischi connessi al trattamento e quali sono le conseguenti misure da adottare per l'effettiva tutela dei dati stessi.

In sintesi l'impresa, ovvero il titolare del trattamento, ha il compito di:
- decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati;
- valutare il rischio che tale trattamento comporta;
- dimostrare di aver adottato le misure tecniche ed organizzative, costantemente aggiornate, tali da garantire un livello di sicurezza adeguato al rischio.

Altrettanto rilevante è il principio della **minimizzazione** ovvero **devono essere trattati solo i dati necessari** per raggiungere le finalità del trattamento. In altri termini i dati raccolti devono essere adeguati e pertinenti rispetto al fine che si intende perseguire e non possono essere raccolti in misura maggiore a quella necessaria.

A questi due principi si ricollegano alcune importanti novità introdotte dal Regolamento, ovvero la *privacy by design* e la *privacy by default*.

Privacy by design ("fin dalla progettazione"): è necessario tutelare i dati sin dalla fase di sviluppo, progettazione, selezione o utilizzo di applicazioni, servizi e prodotti per il trattamento di dati personali. In altre parole, ove il titolare intenda trattare dati altrui, deve già aver previsto un sistema che sin dall'inizio dell'attività, minimizzi la raccolta dei dati e limiti possibili violazioni dei dati raccolti.

La ***privacy by default:*** devono essere adottate misure tecniche e organizzative volte a garantire che vengano trattati solo i dati personali necessari alle finalità perseguite. Ciò comporta l'impostazione predefinita (di *default*) di un trattamento minimo dei dati ovvero il trattamento dei dati personali solo nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario.

- **COSA DEVE FARE L'IMPRESA?**

1) **Mappare** i trattamenti ovvero verificare la sua situazione attuale rispetto al trattamento dei dati personali. Ciò consentirà di avere una fotografia dell'impresa rispetto a:

- le tipologie di trattamenti (ad es. raccolta, archiviazione, etc.);
- le tipologie dei dati trattati (che potranno essere dati personali comuni o sensibili);
- le finalità dei trattamenti (ad esempio la gestione delle relazioni commerciali);
- i soggetti che trattano i dati;
- il flusso dei dati (in entrata e in uscita);
- la durata dei trattamenti;
- la base giuridica del trattamento (contratto, consenso, obbligo di legge).

Con quali strumenti? Check-list dei trattamenti

2) **Individuare le azioni** per essere in regola con la nuova normativa:

- la minimizzazione dei dati (l'impresa dovrà limitarsi a trattare solo i dati strettamente necessari alla finalità perseguita);
- l'identificazione per ogni trattamento della base giuridica (ad es. un contratto o un obbligo legale);
- la revisione della modulistica (informativa, consenso, etc.);
- il controllo delle misure tecnico-organizzative (sono adeguate alla protezione effettiva ed efficace dei dati in base anche al rischio connesso ai tipi di dati (soprattutto sensibili) e al trattamento effettuato?);
- la verifica dell'esistenza di trattamenti automatizzati (ad es. profilazione) che richiedono particolare attenzione e misure di protezione più elevate;
- l'eventuale trasferimento di dati al di fuori dell'UE
- nominare – ove necessario – i responsabili del trattamento.

Con quali strumenti? Misure tecniche ed organizzative (es. adeguata formazione del personale che tratta i dati, misure di sicurezza in termini di accessibilità ai dati, di sicurezza cartacea e informatica); modulo informativa; modulo consenso.

3) **Documentare la conformità** alla nuova disciplina.

Con quali strumenti? Registro dei trattamenti nel quale sono contenute una serie di informazioni relative ai vari trattamenti effettuati (ad es. chi è il titolare o il responsabile, la finalità e la durata, la base giuridica, etc.). Modulistica aggiornata; consenso al trattamento; contratto o un atto di designazione del responsabile del trattamento; procedure specifiche in caso di *data breach* (perdita, distruzione o diffusione indebita dei dati posseduti dall'impresa); procedure in caso di esercizio dei diritti dell'interessato previsti dal regolamento (ad esempio il diritto di accesso, o di rettifica o cancellazione dei dati).

- **COME PUO' FARLO?**

Confartigianato ha realizzato una **serie di strumenti** che possono essere utilizzati da e per le imprese associate. Il Regolamento prevede anche i **codici di condotta** che sono adottati su iniziativa delle Associazioni rappresentative di micro e piccole imprese ed approvate dal Garante. Rappresentano un beneficio per l'impresa che aderisce (sono un elemento per dimostrare la conformità delle misure tecnico-organizzative e sono uno dei criteri per valutare se e quanto sanzionare l'impresa) e contribuiscono alla corretta applicazione del Regolamento.

PAROLE CHIAVE della NUOVA DISCIPLINA della PRIVACY

- **Obbligo di informativa:** nella sostanza l'informativa non cambia. Deve essere chiara e semplice e deve contenere il riferimento alla durata del trattamento e, quando è previsto, del responsabile della protezione dei dati.

- **Consenso dell'interessato per l'utilizzo dei dati comuni:** è necessario acquisirlo (anche se non deve più essere documentato per iscritto) ad eccezione (come oggi) se i dati personali comuni sono utilizzati per eseguire un contratto; per soddisfare un obbligo di legge (ad es. antiriciclaggio); per dati di fonte pubblica (es. dati dell'anagrafe).

- **Consenso esplicito dell'interessato per l'utilizzo di dati sensibili:** è necessario acquisire il consenso esplicito ad eccezione se i dati sensibili sono trattati per la gestione dei rapporti di lavoro e per la sicurezza sul lavoro; per i dati giudiziari in conformità all'articolo 10 del Regolamento.

- **Notificazioni al garante:** non saranno più previste.

- **Registro dei Trattamenti**: Vi è l'obbligo per le imprese con più di 250 dipendenti e per quelle imprese che trattano dati sensibili o giudiziari. E' uno strumento fondamentale anche per disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'impresa ed è indispensabile per la valutazione del rischio. Deve avere forma scritta e deve essere esibito di richiesta al Garante.

- **Valutazione dell'impatto della protezione dei dati**: è introdotta dal nuovo Regolamento ed è da attuare solo quando il trattamento presenta rischi potenzialmente elevati per gli interessati. Consiste nella valutazione dei rischi derivanti dal trattamento dei dati personali per i diritti e le libertà degli interessati e nelle misure per mitigarli.

- **Titolare del trattamento:** l'impresa che ha potere decisionale sull'uso dei dati personali di propria pertinenza.

- **Data Protection Officer (DPO) o Responsabile della Protezione dei Dati:** nuovo organo indipendente di sorveglianza circa l'effettività del sistema realizzato dall'azienda per essere conforme al regolamento. E' obbligatorio in alcuni casi. Il Garante ha pubblicato uno schema di atto di designazione ed ha chiarito quali sono i soggetti privati obbligati alla sua designazione (ad es. sindacati, Caf, Patronati, società che forniscono servizi informatici) e la raccomanda per gli altri casi alla luce del principio di "accountability".