CDS s.r.l.
DIAGNOSTICA STRUMENTALE

Brescia, 20/03/2018

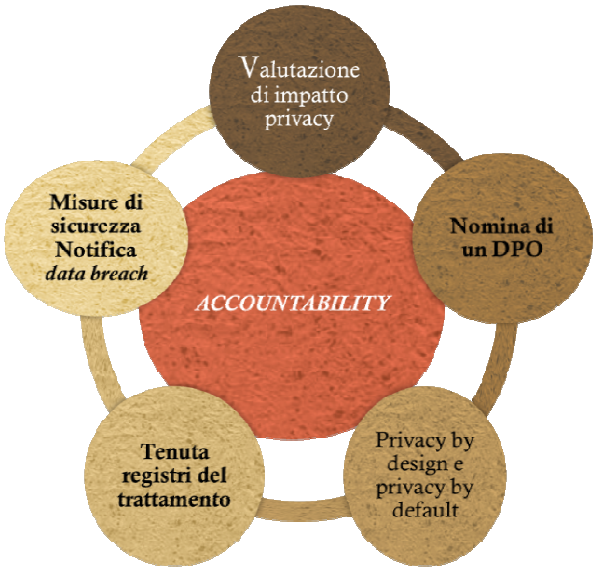
Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il ***Regolamento Generale sulla data protection (GDPR) 2016/679***, che sarà applicabile in tutti gli stati membri, e pertanto obbligatorio per tutte le aziende, a partire dal **25 maggio 2018**.

Il Regolamento introduce una serie di novità in materia di obblighi, diritti e conseguenti sanzioni in caso di inadempimento da parte del Titolare (fino al 4% del fatturato totale annuo dell'azienda o fino ad un massimo di 20 milioni di euro).

## I principali cambiamenti per le imprese

### Il principio di RESPONSABILIZZAZIONE del Titolare

Il Titolare si vede attribuito il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali in relazione alla specificità della propria organizzazione. In quest'ottica la nuova disciplina impone un diverso approccio da parte delle aziende (*Valutazione d'Impatto*, *Privacy by design e default*), prevedendo nuovi adempimenti ed una concreta attività di adeguamento.



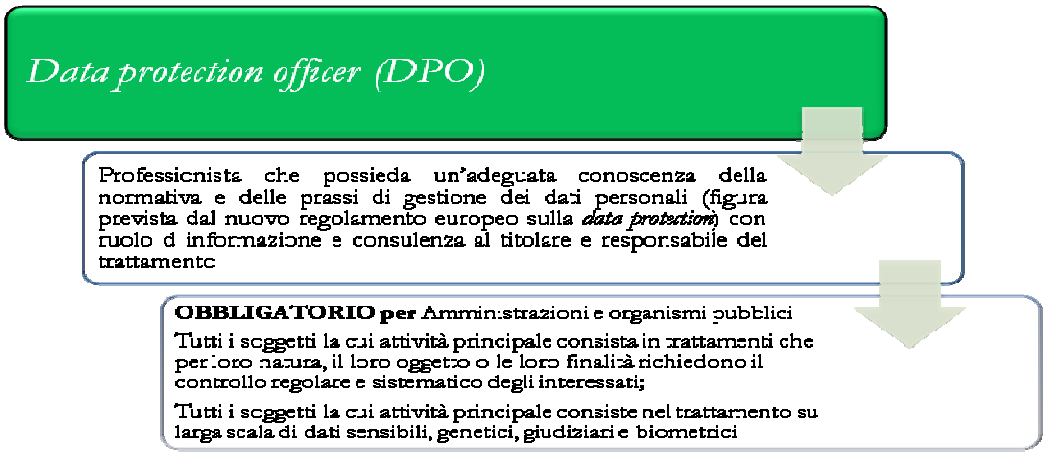

### VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

La valutazione d'impatto sulla protezione dei dati (DPIA) rappresenta il processo

finalizzato a descrivere i trattamenti posti in essere nell'ambito della propria organizzazione, valutarne la necessità e la proporzionalità, individuare i rischi per i diritti e le libertà degli interessati (dai dipendenti ai terzi persone fisiche) così da determinare le misure adeguate per affrontarli.

## IL DATA PROTECTION OFFICER (DPO)

Il Responsabile della protezione dei dati è la nuova figura introdotta dal Legislatore europeo cui spetta la sorveglianza della corretta applicazione del Regolamento; il supporto e collaborazione con il Titolare nell'attuazione della richiamata normativa; la cooperazione con il Garante ed il formale punto di contatto con l'Authority.




## PRIVACY BY DESIGN E PRIVACY BY DEFAULT

***Privacy by design*** significa protezione dei dati fin dalla progettazione ovvero ridurre al minimo il trattamento dei dati mediante misure tecniche ed organizzative quali, ad esempio, la loro pseudonimizzazione.
***Privacy by default*** significa invece che la tutela della protezione del dato deve diventare l'impostazione predefinita, pertanto il Titolare del trattamento dovrà adottare misure tecniche ed organizzative adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento.

## TENUTA DEI REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, il Garante raccomanda a tutti i Titolari di trattamento, a prescindere dalle dimensioni dell'organizzazione, l'adozione di tale registro e, in ogni caso, di compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.
L'indicato registro deve contenere, tra l'altro, l'individuazione del Titolare, le finalità del trattamento, la descrizione delle categorie degli interessati e delle categorie dei dati trattati, nonché la descrizione delle misure di sicurezza adottate.

## MISURE DI SICUREZZA

Come anticipato in tema di *accountability*, il Titolare dovrà disegnare e gestire la sicurezza nell'ambito della propria organizzazione, avendo cura di modellarla sulla propria struttura. In questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva (la pseudonimizzazione e la cifratura dei dati personali; capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento).

## NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI

A partire dal 25 maggio 2018, il Titolare del trattamento dovrà notificare al Garante le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto laddove ritenga probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. L'indicata notifica dovrà pertanto essere subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

## LE SANZIONI

Il Regolamento prevede un adeguamento al rialzo delle sanzioni amministrative per il Titolare e il Responsabile del trattamento in caso di violazione delle norme in materia di privacy. Il tetto massimo delle sanzioni è previsto nella misura di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.


Per ogni ulteriore informazione CDS resta a disposizione con i suoi consulenti al numero 030/2429612.