10 step per allinearsi al Reg.Ue 679/2016 in materia di privacy e data protection

1) **Conoscenza del nuovo Regolamento**

   Il Reg. 679/2016 sostituirà in toto la dir 95/46/CE: si tratta di un provvedimento più complesso rispetto alla Direttiva e che arriva (dopo oltre 20 anni) a regolare una realtà sostanzialmente diversa da quella del '95 e sempre più digitale. Occorre capirne i punti cardine e la ratio di fondo, nonché verificare che chi opera all'interno della propria struttura abbia consapevolezza di tale evoluzione.

2) **Analisi dei dati trattati**

   Occorre mappare con esattezza *quali dati* si trattano, *perché* si trattano e *come* si trattano.

   Il Regolamento infatti richiede, in sostanza, di effettuare una analisi del rischio dei dati trattati, per definire quali misure adottare al fine di tutelare i diritti degli interessanti, proteggendo i loro dati e gestendo i rischi ineliminabili.

3) **Revisione della Informativa**

   Il nuovo Regolamento si incardina su un principio (in parte) nuovo: l'interessato deve avere il controllo dei propri dati (considerando n. 6). Sotto questo profilo appare chiaro come l'informativa deve essere chiara, completa ed esaustiva: con la nuova disciplina potranno essere usate anche le icone.

   Da rivedere quindi le informative "copia-incolla": la logica del sistema richiede che l'informativa sia lo strumento principe per permettere all'interessato di *sapere* e, quindi, di *decidere* se e *come* permettere il trattamento dei dati.

4) **Verifica dell'impatto dei nuovo diritti del soggetto interessato**

   La nuova disciplina non solo ribadisce ed amplia la tutela dei diritti dell'interessato già esistenti, ma ne crea dei nuovi. Oltre infatti ai diritti conoscitivi dell'informativa ed accesso, sono disciplinati i c.d. diritti di controllo, quali la limitazione al trattamento, la revoca del consenso, il diritto all'oblio, ed altresì il diritto alla portabilità dei dati.

   E' necessario quindi verificare le procedure interne atte a dare risposta ove l'interessato azioni i suoi diritti e, per quanto riguarda in particolare, il (nuovo) diritto diritto alla portabilità valutare una eventuale riorganizzazione interna, atta a consentire all'interessato di poter ricevere i propri dati in formato strutturato, di uso comune e leggibile.

5) **L'acquisizione del consenso**

   Il consenso non è più scritto o verbale, ma per tutti libero (non condizionato), specifico (uno per ogni finalità), inequivocabile (certo) ed espresso. Per chi tratta poi dati sensibili deve essere anche "esplicito". Poiché, poi, è in capo al titolare la prova di aver acquisito correttamente il consenso, occorre verificare

con precisione il rapporto tra chiarezza della informativa e modalità di acquisizione dei diversi consensi a seconda delle diverse finalità.

6) **Il rispetto dell'accountability**

L'accountability è principio cardine del nuovo sistema: il titolare non è chiamato infatti al mero adempimento di un elenco di obblighi, ma è tenuto oggi a valutare i suoi trattamenti sotto il profilo del rischio, ad implementare le misure idonee e necessarie, a gestire il rischio residuo e, soprattutto, a dimostrare *perché* ha scelto quello misure (piuttosto che altre).

Cambia quindi totalmente la prospettiva: da reattiva a pro-attiva.

Occorre quindi rivedere il proprio processo interno di gestione del dato sotto questa nuovo lente

7) **La privacy by design, il registro dei trattamenti, la valutazione di impatto**

il Regolamento introduce poi nuovi adempimenti che occorre sin da oggi cominciare a capire ed ad implementare: una riorganizzazione del servizio o una progettazione del prodotto che tenga conto della privacy sin dall'inizio (privacy by design e by default - art. 25), la predisposizione del registro delle attività di trattamento ove richiesto (art. 30), la valutazione di impatto (art. 35) richiesta nello specifico per il trattamento dei dati sanitari su larga scala.

8) **Data Protection Officer**

E' una figura nuova, che svolge in parte attività di consulenza e formazione ed in parte attività di controllo. E' tenuto ad avere conoscenza sul nuovo Regolamento e sugli atti interpretativi (corte di giustizia e WP 29) nonché competenza di natura tecnologia. Inoltre, proprio in ragione

dei suoi compiti di controllo, non può essere in posizione di conflitto di interessi.

In ragione di quanto sopra, nelle Linee Guida del WP29 si ammette espressamente la possibilità che l'incarico sia conferito ad enti giuridici che possano vantare una multiprofessionalità.

9) **Il trasferimento di dati**

Occorre accertarsi dove sono i propri dati e come vengono trattati, specie nel caso di cloud o di uso di app. E' poi necessario verificare se il paese dove eventualmente i dati risiedono o sono trasferiti ha un accordo con la UE, e quali sono i termini.

10) **Data breach**

Esteso a tutti i trattamenti ed a tutti i titolari l'obbligo di comunicare eventuali violazione dei dati o del sistema (meccanismo già obbligatorio in area sanitaria per il Dossier Sanitario). Occorre quindi predisporre idonea procedura interna.