di *Giovanna Raffaella Stumpo*[i]

Il 25 Maggio prossimo, il GDRP (*General Data Protection Regulation*) – Regolamento del Parlamento europeo e del Consiglio 27 aprile 2016 n. 697 (*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati)* – anche solo Il Regolamento - diventerà efficace e vincolante nei 28 Stati Membri (SM) dell'Unione Europea, con efficacia abrogativa della Direttiva n. 95/46/CE (*regolamento generale sulla protezione dei dati*) e con conseguente caducazione - per l'Italia – dell'attuativo Dlgs. 30 giugno 2003 n. 196 (*Codice in materia di protezione dei dati personali*).

In assenza di un quadro normativo nazionale applicabile ed a fronte di un Atto regolamentare di rango sovranazionale di diretta applicabilità, dal 25 del mese prossimo, fatto salvo il sopravvenire di nuove regole che, come da previsione dello stesso GRDP sono rimesse alla determinazione degli SM (cfr. Capo II, art. 6 comma 3 lett. b)) e delle Autorità competenti (cfr. Sez. 1 e 2 Capo VI, artt. da 51 a 59; Capo VII, artt. da 68 a 76)), per tutti i principali diversi Operatori di mercato europeo - Aziende, PA e Studi - che, nell'esercizio del *business* ed in particolare nell'attività di produzione /erogazione di beni /servizi trattano dati personali di Interessati - persone fisiche- con ricorso in tutto/in parte a strumenti elettronici e non (cfr. Capo I art. 2 comma 1), e con impatto in ambito UE (cfr. Capo I, art. 3) e che si qualificano come Titolari del trattamento ai sensi dell'art. 4, punto 7), si impongono le previsioni programmatiche e di dettaglio, di cui al GRDP.
Con obbligo di dare corso – senza ulteriore dilazione - ad una serie di adempimenti operativi di non poco conto, sul piano sia delle scelte di metodo, sia di organizzazione; e che richiedono al Titolare di dotarsi di una serie di figure di riferimento dell'Organigramma privacy (i.e. Responsabile/i interno/i ed esterno/i, Addetto/i al trattamento, e sussistendone i presupposti - Responsabile della protezione dei dati o DPO – *Data Protection Officer*), con oneri di nomina, istruzione, delega e formazione adeguati al ruolo di ricoprire ed ai compiti da attuare, e secondo le previsioni dello stesso Regolamento.

<u>Quali sono i primi adempimenti su cui focalizzare l'attenzione metodologico organizzativa?</u>

Salvo le eccezioni espressamente previste per alcuni adempimenti (in particolare per le PMI), a chi, all'interno dell'Organizzazione effettua le determinazioni circa "*finalità e mezzi del trattamento*" – e, quindi, conseguentemente si qualifica quale "Titolare"-, il GRDP impone l'osservanza del principale obbligo "di responsabilizzazione" (cfr. Capo II, art.5 comma 2); che fa leva sul comportamento attivo (cfr. Capo IV, Sez. 1) del Vertice decisorio con riferimento ai seguenti principi ispiratori del nuovo dettato regolamentare europeo sulla tutela del dato:

- ***accountability*** (i.e. necessità da parte del Titolare di dimostrare l'adozione di politiche privacy e misure adeguate alla tutela dei diritti e degli interessati dell'Interessato, in conformità al dettato regolamentare);
- ***privacy by design*** (i.e. necessità di adozione da parte del Titolare di misure tecnico – organizzative adeguate a protezione dei dati oggetto del trattamento, fin dalla progettazione ed anche nell'atto del trattamento);
- ***privacy by default*** (i.e. necessità per il Titolare, di garantire che i dati vengano trattati solo per finalità previste e per il tempo strettamente necessario a tali finalità).

Per dare corretta attuazione al Regolamento, il Titolare *"….è tenuto a mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*"; rischiandosi, in difetto di ciò, di incorrere in sanzioni amministrative pecuniarie particolarmente rilevanti, posto che – impregiudicate nuove sanzioni disposte con regolamentazione nazionale (cfr. Capo VIII, art. 84 comma 1), allo stato e per disposto del Regolamento, le stesse possono anche arrivare fino ad un massimo di 20 milioni di euro / fino al 4% del fatturato mondiale totale annuo (cfr. Capo VIII, art. 83).

Il quadro dei principali adempimenti

Per essere *compliant*, operativamente, al Titolare si richiede principalmente di:

1. allinearsi nell'organizzazione del trattamento del dato, ai principi di cui al Capo II (in particolare artt. 5 e 6) formalizzando anche una specifica "*privacy policy*";
2. adottare metodologia e strumenti idonei a garantire agli Interessati, il possibile esercizio dei diritti di cui al Capo III (in particolare artt. da 12 a 22); con informativa circa i mezzi di reclamo e ricorso, ugualmente a disposizione (cfr. artt. 77 – 79);
3. organizzare il "quadro di informative e consenso" al trattamento del dato, secondo il disposto degli artt. da 7 a 9, ivi compresa la comunicazione collegata alla "trasferibilità dei dati" intra UE e/o verso Paesi terzi e/o Organizzazioni internazionali ed organizzando – per una tale evenienza - misure di tutela adeguate (cfr. Capo V artt. da 44 a 50);
4. provvedere alla tenuta, con corretta compilazione ed aggiornamento del registro dei trattamenti (cfr. Capo IV art. 30); regolamentando anche le modalità di cooperazione con le competenti Autorità di controllo (cfr. Capo IV, art. 31) per il caso esercizio di poteri ispettivi, di controllo e/o richiesta informazioni ed evidenze;
5. dotarsi di misure di sicurezza adeguate ai rischi sottesi al trattamento di cui all'art. 32; organizzando per i casi di c.d. "*data breach*", le modalità di notifica delle violazioni subite alla competente Autorità di controllo nazionale e, -sussistendone i presupposti – della comunicazione anche all'Interessato pregiudicato dalla violazione (cfr. Capo IV, art. 34);
6. sussistendone di presupposti ed in particolare per i trattamenti con ricorso alle nuove tecnologie con alto rischio per i diritti e le libertà dell'Interessato – effettuare la preventiva valutazione d'impatto sulla protezione dei dati (cfr. Capo IV, art. 35); organizzando anche il processo di consultazione preventiva della competente Autorità di controllo, per le ipotesi contemplate all'art. 36;
7. costruire l'"Organigramma privacy", ed in particolare organizzare il supporto e la collaborazione attiva di una pluralità di figure chiave per la gestione degli adempimenti privacy, tra cui in particolare:
   - sussistendone i presupposti di normativa (cfr. art. 3 par. 2 e art. 27) - il Rappresentante stabilito, a norma dell'art. 4 punto 17);
   - il Responsabile/i del trattamento a norma dell'art. 4 punto 8);
   - gli Addetti al trattamento (cfr. art. 4 punto 10 e art. 29) e
   - sussistendone i presupposti di normativa (cfr. art. 37 comma 1 lett. da a) a c)) - il Responsabile della protezione dei dati (il DPO – *Data Protection Officer*); organizzando anche gli adempimenti di informativa/comunicazione esterna obbligatori, quanto alle nomine effettuate;
8. realizzare – con il supporto e per il tramite delle figure in Organigramma, un adeguato SGP (Sistema di Gestione Privacy) documentabile e sorretto da specifiche procedure ed istruzioni

operative formalizzate e/o supportate da ausili di tipo informatico (ad es. SW dedicati per le registrazioni, analisi, misure e relative evidenze).

Le figure in Organigramma ed il problema delle qualifiche delle competenze

In relazione all'Organigramma privacy, si richiede al Titolare di procedere con atti di designazione, nomina ed istruzione, previa valutazione delle effettive competenze dei soggetti scelti; in modo da poter fornire "garanzie sufficienti" a comprovare la capacità di assolvere gli adempimenti operativi sia in conformità delle regole imposte dallo stesso Regolamento, sia a garanzia della tutela dei diritti degli Interessati.

Il tema della "qualifica delle competenze", si pone quindi in tutta evidenza, per le scelte di designazione e nomina in capo al Titolare. E ciò, in particolare, per quanto attiene:
a) al Responsabile del trattamento (da designarsi con i compiti di cui a specifico contratto da formalizzare *ad hoc ex* art. 28 comma 3), posto che il Regolamento dispone che: "*qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garanzia della tutela dei diritti dell'Interessato*" (cfr. Capo IV art. 28 comma 1) e,
b) al DPO (da scegliersi tra un dipendente o un soggetto esterno in base a specifico contratto di servizi, sussistendo i presupposti per la designazione di cui all'art. 37 comma e per i compiti di cui all'art. 39), dato che sempre il Regolamento prescrive di scegliere la figura nel ruolo "*in funzione delle qualità professionali ed in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità*" – operativa -, "*di assolvere*" – minimamente (cfr. art. 38 comma 6) "*i compiti di cui all'art. 39*" (i.e. informativa e consulenza in merito agli obblighi del Regolamento; sorveglianza dell'osservanza del Regolamento, della privacy policy, del quadro delle responsabilità ed autorità allocate e dei doveri di sensibilizzazione e formazione del personale che partecipa ai trattamenti; pareri - su richiesta- in merito alla valutazione d'impatto, sorvegliandone lo svolgimento; cooperazione con l'Autorità di controllo; fungere da punto di contatto per la predetta Autorità e gli Interessati); con correlata presa in considerazione del Titolare, per la figura nel ruolo di DPO, anche della sua capacità valutativa dei rischi inerenti alle attività di trattamento "*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo"* (cfr. art. 39 comma 2).

Come può il Titolare esercitare positivamente l'onere della prova, di aver effettuato una "scelta adeguata" e *compliant* con i requisiti del Regolamento, in relazione alla corretta scelta, nella designazione delle due figure principali di cui all'Organigramma privacy?

In proposito si ricorda che:
i) – quanto al Responsabile del trattamento- ai sensi e per gli effetti dell'art. 28 comma 5 "*l'adesione da parte del Responsabile del trattamento ad un codice di condotta approvato di cui all'art. 40 o a un meccanismo di certificazione approvato di cui all'art. 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai par. 1 e 4 del presente articolo";*
ii) – quanto al DPO - i requisiti di conoscenza, competenza e capacità non specificati direttamente dal Regolamento, sono regolamentati nelle Linee Guida sui Responsabili della protezione dei dati del Gruppo di lavoro art. 29 per la protezione dei dati n. 16/IT - WP243 rev. 01;

iii) a livello di normazione tecnica, esiste la norma nazionale UNI 11697 (*Attività professionali non regolamentate Profili professionali relativi al trattamento ed alla protezione dei dati personali)* che declina in modo specifico i requisiti di qualificazione, conoscenza, abilità e competenza delle seguenti nuove figure professionali: Responsabile della protezione dei dati – DPO; *Manager* Privacy, Verificatore Privacy, *Specialist* Privacy.

Allo stato si attende la conversione della predetta norma nazionale UNI 11697 a norma europea CEN.

ACCREDIA ed il Garante privacy, sul punto e con comunicato stampa del 18 Luglio 2017 hanno in particolare richiamato l'attenzione degli Operatori di mercato sulla necessità– nell'allineamento agli obblighi di adeguamento al Regolamento e con particolare in attinenza sia alle misure tecniche ed organizzative, sia alla qualifica delle competenze di cui trattasi - di attendere la definizione di requisiti comuni per la conformità delle certificazioni, sottolineando come vi siano collaborazioni in corso, al fine di cercare di rispettare la scadenza di diretta applicabilità, del 25 Maggio 2018.

Nel mentre, entrambi i soggetti istituzionali coinvolti, come da comunicato sopra citato, rimarcano tuttavia che "…..*al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le Parti Interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi conformi agli artt. 42 e 43 del Regolamento n. 679/2016/UE, poiché devono ancora essere determinati i "requisiti aggiuntivi", ai fini dell'accreditamento degli Organismi di certificazione ed i criteri specifici di certificazione*" (RIPRODUZIONE RISERVATA).

[i] ***Avvocato del Foro di Milano, Giornalista pubblicista, Esperta in discipline strumentali all'esercizio della professione forense.***