IL REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: TRA APPROCCI INNOVATIVI E ACCOUNTABILITY

DI MARIANNA QUARANTA

1. Come ormai noto, il 27 aprile 2012 la Commissione Europea ha presentato un Regolamento per l'aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. (d'ora innanzi anche GDPR)

Il regolamento UE, essendo un atto *self executive*, ai sensi dell'articolo 288 del Trattato sul Funzionamento dell'Unione Europea, è direttamente ed immediatamente esecutivo e non necessita di recepimento da parte degli Stati membri, cosicché a decorrere dal 25 maggio 2018, la normativa su citata diventa immediatamente applicabile anche nello Stato italiano.

Il tema della tutela dei dati personali è stato affrontato dal legislatore italiano nella primitiva legge 675 del 1996 poi abrogata dal decreto legislativo 196 del 30 giugno 2003, recante il cosiddetto "Codice della Privacy". (d'ora innanzi Codice)

Si tratta di due pietre miliari che hanno posto le fondamenta nel nostro ordinamento affinché fosse riconosciuta dignità al diritto alla "privatezza" e che hanno individuato, in capo al titolare del trattamento, un sistema di adempimenti che consentisse, una volta applicato, di ritenere correttamente eseguito il trattamento dei dati.

In particolare, l'impianto normativo disegnato dal Codice della Privacy consentiva di individuare, con un sufficiente grado di dettaglio, le misure di sicurezza che, secondo il legislatore, potevano considerarsi "necessarie e sufficienti" ai fini della correttezza del trattamento. Segnatamente, come noto, l'allegato B del citato D.Lgs.196/2003 prevedeva per l'appunto la regolamentazione e l'elencazione delle misure minime di sicurezza da applicare, specie con riferimento ai trattamenti di tipo telematico e informatico.

Di qui la previsione di un documento programmatico sulla sicurezza (DPS) la cui adozione ed aggiornamento non solo erano obbligatori, ma anche suscettibili di sanzione sia in sede civile che penale.

Il superamento della obbligatorietà di talune misure sembrava declinare un sistema che alleggerisse il titolare del trattamento, in realtà, il nuovo Regolamento Europeo è impostato sul sistema cosiddetto dell'*accountability*, ovvero, la normativa stabilisce che sia il titolare del trattamento ad individuare quelle misure che possano, in maniera adeguata, tutelare gli interessati al trattamento.

Questa impostazione sbilancia fortemente l'asse a carico del titolare del trattamento il quale se, da un lato, sembra alleggerito del sistema degli adempimenti, dall'altro, proprio per la valutazione di congruità a lui rimessa del sistema adottato, impone una *risk analysis* che deve essere eseguita, onde individuare quelle criticità nella *governance* del trattamento dei dati che potrebbero determinare lesioni dei diritti dell'interessato.

Ma procediamo con ordine.

2. Anzitutto, va dato atto che il nuovo Regolamento Europeo ribadisce la centralità di un principio, sposato dal vecchio Codice, ovvero quello della **liceità del trattamento**, difatti, all'art. 6 prevede che vi sia sempre un'espressione di consenso da parte dell'interessato, ovvero, che il consenso non sia necessario solo per l'adempimento di obblighi contrattuali o laddove il trattamento sia prodromico all'esercizio degli interessi vitali della persona interessata o di terzi od ancora, che vi sia un interesse legittimo prevalente del titolare o di terzi rispetto a quello dell'interessato cui i dati vengono comunicati.

Naturalmente, per i **dati sensibili,** il **consenso** deve essere **esplicito** ed, in particolare, il nuovo Regolamento ribadisce l'importanza della raccolta del consenso informato, laddove, vi siano trattamenti automatizzati, specie ove sia prevista la profilazione. In tutti i casi, il consenso deve essere libero specifico, informato ed inequivocabile, mentre, non è ammesso il consenso tacito, presunto, né con l'uso di caselle spuntate su modulo.

Il consenso che sia stato raccolto precedentemente al 25 maggio 2018 resta valido, purché, esso presenti caratteristiche testé individuate.

Giova rimarcare che, ai sensi dell'art. 7.2., la richiesta di consenso deve essere chiaramente distinguibile rispetto ad altre richieste o dichiarazioni somministrate di volta in volta, all'interessato e la formulazione utilizzata deve essere comprensibile, semplice e chiara.

Va, infine, dato atto che la valutazione sul bilanciamento tra legittimo interesse del titolare o di un terzo ed i diritti e libertà dell'interessato non spetta all'Autorità, nello specifico al Garante per la protezione dei dati personali, ma diventa essa stessa compito del titolare del trattamento in ossequio al principio di responsabilizzazione introdotto dal nuovo pacchetto protezione dati.

Trovano conferma anche le prescrizioni già adottate dall'Autorità nei provvedimenti in materia di bilanciamento degli interessi, in particolare, rispetto ai trattamenti che hanno ad oggetto **dati biometrici** e segnatamente le cautele già prescritte nella fase di *enrollment* e nella conservazione del dato su supporti che restino nella disponibilità dell'interessato. Nonché, le prescrizioni, già adottate dal Garante, in materia di **videosorveglianza** con particolare riferimento ai tempi di tenuta delle immagini e all'adeguatezza dell'informativa, anche mediante l'uso di idonea cartellonistica.

3. Con riferimento all'**informativa**, il Regolamento presenta contenuti più ampi rispetto al Codice, in particolare, nell'informativa devono sempre essere specificati i dati di contatto del Responsabile per la protezione dei dati e, laddove previsto, del Data Protection Officer (DPO). I contenuti sono più ampi rispetto a quelli descritti dal Codice così, esemplificando, deve essere specificata la base giuridica del trattamento e, laddove i dati personali sono trasferiti in paesi terzi, vanno specificati la modalità e gli strumenti del trattamento.

Il titolare dovrà, altresì, darsi cura di specificare (nell'informativa) il periodo di conservazione dei dati ed i criteri seguiti per stabilire tale periodo di conservazione, nonché, il diritto di presentare reclamo all'Autorità di controllo.

Inoltre, come si è già accennato, se il trattamento comporta processi decisionali automatizzati, l'informativa deve specificarlo, indicando, altresì, la logica di tali processi e le eventuali conseguenze sull'interessato.

Normalmente, l'informativa viene somministrata contestualmente all'acquisizione del consenso: è possibile, però, che non sia così. In tal caso, essa deve essere fornita in un tempo ragionevole che non può, in ogni caso, superare un mese dalla raccolta. La somministrazione avviene di norma per iscritto, ovvero, in formato elettronico soprattutto nel contesto dei servizi *on line*, ma già il Codice sottolineava la possibilità che l'informativa fosse resa in forma sintetica attraverso

l'utilizzo di icone. Secondo il nuovo Regolamento le icone utilizzate a tal fine dovranno essere identiche per tutta l'Unione Europea e saranno definite dalla Commissione Europea.

Sempre con riferimento all'informativa, va, infine, dato atto che la normativa in commento supporta chiaramente il concetto di "**informativa stratificata"** già, più volte, adottato dal Garante per la protezione dei dati personali.

In particolare, viene favorita l'adozione di informative che man, mano che il trattamento diventa più pervasivo, informano l'interessato delle dinamiche del trattamento.

4. Anche l'area dei **diritti degli interessati** è stata revisionata con l'introduzione di correttivi significativi. Con riferimento al diritto di accesso si sottolinea che deve essere dato riscontro all'interessato entro un mese dalla richiesta, estendibile a tre mesi in caso di particolare complessità. In caso di diniego, deve essere, comunque, dato riscontro all'interessato entro un mese dalla richiesta.

In linea con lo spirito di **autoresponsabilizzazione** dell'intero Regolamento, spetterà al titolare del trattamento valutare la complessità del riscontro da dare all'interessato e sarà sempre il titolare a stabilire l'ammontare dell'eventuale contributo da richiedere all'interessato per le copie dei dati e qualsiasi altro costo sostenuto per espletamento della richiesta compresi i costi amministrativi sostenuti.

Il riscontro dovrà avvenire in forma scritta, ma potrà essere predisposto anche attraverso l'uso di strumenti elettronici che favoriscano l'accessibilità, benché, il riscontro sia da rinvenirsi sempre dal titolare del trattamento: anche il responsabile è tenuto a collaborare con il titolare ai fini del miglior esercizio dei diritti degli interessati.

Particolarmente interessante per il suo carattere innovativo, in quanto sancisce e ratifica quanto già la giurisprudenza aveva appurato in via interpretativa, è l'introduzione all'articolo 17 del cosiddetto **diritto all'oblio**: esso si configura come il diritto alla cancellazione dei propri dati personali in forma rafforzata. Difatti, viene introdotto l'obbligo al paragrafo 2, per i titolari del trattamento che hanno reso pubblici i dati dell'interessato pubblicandoli, ad esempio, attraverso un sito web, di informare della richiesta di cancellazione pervenuta dall'interessato

altri titolari che trattano i medesimi dati personali cancellati, compresi qualsiasi link, copia o riproduzione.

Tale previsione interessa, in maniera significativa, soprattutto coloro che diffondono notizie *on line* ovvero che usino *blog* o testate giornalistiche telematiche che con la diffusione massiva dei contenuti, pressoché illimitata, sono i soggetti prioritariamente destinatari dell'incombente (fatto salvo il bilanciamento con altri diritti ed interessi, si pensi al diritto di cronaca, al diritto alla conservazione per finalità di ricerca, etc.).

Sempre in prospettiva innovativa va letto l'articolo 18 del Regolamento nella parte in cui consente **limitazioni al trattamento** dei dati. Si tratta di una facoltà ben più significativa ed ampia rispetto al mero blocco del trattamento di cui all'articolo 7, comma 3, lettera a) del Codice, difatti, tale diritto è esercitabile non solo laddove ricorrono violazioni dei presupposti di liceità del trattamento, ma anche laddove l'interessato chieda la rettifica del dato o si oppone al trattamento.

Allorquando, pervenga una segnalazione da parte del titolare relativa alla limitazione del trattamento, la normativa in commento prevede che il dato personale sia contrassegnato in attesa di determinazioni ulteriori. Pertanto è opportuno che i titolari del trattamento nel predisporre il sistema di verifica dei dati sia esso elettronico oppure no, adottino misure idonee a tale scopo.

Nell'ambito delle innovazioni introdotte ai diritti dell'interessato va, altresì, segnalata la **portabilità del dato**.

Si tratta di una previsione non sconosciuta ai consumatori, in quanto, già introdotta in materia di telefonia mobile con la cosiddetta *number portability* e consente all'interessato di mantenere il consenso, così come prestato, rispetto al dato trattato anche verso altri interlocutori.

Naturalmente, la previsione ha senso solo con riferimento ai trattamenti automatizzati, pertanto, se ne esclude l'applicabilità agli archivi o ai registri cartacei.

Sono portabili solo i dati trattati acquisito con il consenso dell'interessato, e quei dati che siano stati raccolti in base ad un contratto stipulato con l'interessato, in altri termini, vengono esclusi i trattamenti che si fondano sul mero interesse pubblico o sull' interesse legittimo del titolare.

In ogni caso, ai fini della portabilità, il titolare deve essere in grado di trasferire direttamente i dati portabili ad un altro titolare indicato dall'interessato, ma sempre che ciò sia tecnicamente possibile. Sulla portabilità del dato il Workshop 29 ha pubblicato delle linee guida dove vengono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati. In merito, il Gruppo di lavoro sottolinea come la trasmissione dei dati da un titolare all'altro preveda che si utilizzino *formati interoperabili*, cosicché i titolari dovrebbero adottare, fin da subito, misure idonee a produrre i dati richiesti con un formato interoperabile e facilmente condivisibile.

5. Se queste, in estrema sintesi, sono le prescrizioni dettate per la tutela dell'interessato il Regolamento non manca di intervenire sui soggetti che dal lato attivo presiedono al trattamento. In particolare, si è già detto, che con il sistema dell'*accountability* il regime delle responsabilità si sbilancia fortemente a carico del titolare del trattamento, il quale se, da un lato, può individuare, in base al tipo di trattamento eseguito e alla sua struttura, le migliori modalità per l'esecuzione del trattamento e la raccolta del dato, dall'altro, deve preoccuparsi di dimostrare di aver adottato misure sufficienti sotto il profilo tecnico ed organizzativo, adeguate a consentire il rispetto dei diritti dell'interessato.

Un supporto significativo, in tal senso, viene offerto dal responsabile del trattamento il quale dovrà essere incaricato dal titolare che dovrà darsi carico di specificare, in maniera chiara, i compiti specifici attribuitigli. Nel far ciò, il titolare del trattamento dovrà preoccuparsi di fornire tutte le indicazioni e le prescrizioni che il responsabile del trattamento dovrà porre in essere. In particolare, attraverso un contratto o altro atto giuridico conforme al diritto nazionale, il titolare del trattamento dovrà preoccuparsi di evidenziare, oltre alle istruzioni e alle misure tecniche ed organizzative adeguate a consentirne il rispetto, anche di specificare la natura, la durata e la finalità del trattamento o dei trattamenti, anche diversi, eventualmente assegnati al responsabile.

È possibile, diversamente da quanto previsto per il passato, che vi sia la nomina da parte del responsabile del trattamento, di sub - responsabili per specifiche attività sempre che tale (sub) nomina avvenga nel rispetto degli obblighi contrattuali dal primo assunti. Questi risponderà, dinanzi al titolare, dell'eventuale

inadempimento del sub - responsabile anche ai fini del risarcimento di eventuali danni, a meno che non dimostri che l'evento dannoso non gli è in alcun modo, imputabile.

I responsabili del trattamento, ai sensi dell'articolo 30, del Regolamento in commento sono tenuti a predisporre il **registro delle attività di trattamento -** su cui si rinvia *infra* – eseguite; essi devono, altresì, provvedere all'adozione di idonee misure tecniche ed organizzative, onde garantire la sicurezza dei trattamenti. Il responsabile del trattamento dovrà, altresì, preoccuparsi di impartire le dovute istruzioni agli incaricati al trattamento, ovvero, a coloro che materialmente eseguono il trattamento, seguendo le prescrizioni impartite dal titolare e dal suo responsabile.

Invero, la normativa europea non prevede, in maniera espressa, la figura dell'incaricato al trattamento, così come avveniva per il Codice, ma non ne esclude la presenza, in quanto, fa riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

In altri termini, implicitamente riconosce queste figure per le quali, in mancanza di diverse prescrizioni, possono valere le indicazioni già previste dal Codice.

Per agevolare il compito non semplice del titolare del trattamento e del suo responsabile di dare atto di aver adottato misure adeguate, il Regolamento prevede l'adesione a **codici deontologici,** ovvero, l'adesione a **schemi di certificazione** che possano aiutare il responsabile del trattamento a dimostrare di aver adottato le cautele per eseguire, in sicurezza, il trattamento affidatogli. Allo stato, il Garante sta valutando la diffusività dei codici, già attualmente vigenti per alcune tipologie di trattamento, rivisti alla luce dei requisiti fissati dal Regolamento all'articolo 40, mentre, non vi sono ancora "schemi di certificazione" (Art. 42) per i quali occorre l'intervento del legislatore che dovrà stabilire le modalità di accreditamento dei soggetti certificatori.

6. La responsabilizzazione dei titolari e dei responsabili del trattamento poggia sull'adozione di comportamenti proattivi che dimostrino la concreta applicazione delle misure finalizzate ad assicurare la corretta attuazione del regolamento.

Si tratta di una rivoluzione copernicana che ribalta sul titolare del trattamento la scelta delle modalità ritenute più idonee a garantire un trattamento efficace e sicuro.

Tra i criteri che il Regolamento ha sintetizzato, a vantaggio del titolare, il primo è quello di cui all'articolo 25, dove si fa riferimento al cosiddetto *data protection by default and by design*, ossia, alla necessità di configurare il trattamento, prevedendo, fin dall'inizio, le garanzie indispensabili al fine di tutelare, in maniera adeguata, i diritti degli interessati, tenendo conto del contesto complessivo in cui il trattamento si colloca e dei rischi che esso pone alla libertà e ai diritti degli interessati nel rispetto di quanto sancito dal GDPR.

Le scelte effettuate dal titolare devono essere fatte a monte e, pertanto, si richiede un'analisi preventiva ed un impegno applicativo da parte di titolari che devono darsi carico della predisposizione di **attività specifiche e dimostrabili**.

Nella valutazione dei rischi, il titolare del trattamento dovrà valutare l'impatto negativo che il medesimo ha sulle libertà e sui diritti degli interessati, secondo quanto previsto ai considerando 75 e 77 del Regolamento, naturalmente, tale impatto dovrà essere analizzato attraverso un idoneo processo di valutazione, la cosiddetta *Risk Analysis* descritto agli articoli 35 e 36.

Tale processo di valutazione dovrà tener conto dei rischi noti o di quelli ipotizzabili ed evidenziabili con la conseguente adozione di misure di sicurezza tecniche e organizzative che consentano di mitigare tali rischi.

All'esito della valutazione dei rischi, il titolare potrà decidere in autonomia se iniziare il trattamento, ritenendo, in tal caso, di aver adottato tutte le misure di sicurezza necessarie e sufficienti a mitigare gli effetti dei rischi, ovvero, potrà, in via preventiva, consultare il Garante per la protezione dei dati personali, onde, ottenere indicazioni su come gestire il rischio residuale.

In tal caso, l'Autorità non avrà il compito di autorizzare il trattamento, ma di indicare eventuali ulteriori misure correttive da adottare. In altri termini, l'Autorità interverrà principalmente *ex post* e ciò spiega perché, a partire dal 25 maggio 2018, alcuni istituti come, ad esempio, quello della notifica di taluni trattamenti, ovvero, la verifica preliminare di taluni altri di cui all'articolo 17 del

Codice, sono superati a vantaggio degli obblighi di tenuta del registro dei trattamenti da parte del titolare e del responsabile del trattamento.

In ogni caso, è fatto obbligo a tutti i titolari e responsabili di trattamento, eccetto gli organismi con meno di 250 dipendenti e sempre che non effettuino trattamenti a rischio, di tenere un registro delle operazioni di trattamento i cui contenuti sono specificati all'articolo 30 del GDPR.

Si tratta di uno strumento che consente di predisporre all'interno dell'azienda, di un quadro aggiornato dei trattamenti in corso ed è indispensabile per ogni valutazione ed analisi del rischio.

Il registro può avere forma scritta anche elettronica e deve essere esibito su richiesta del Garante, ovvero, dei suoi ausiliari, consentendo all'Autorità di supervisionare il trattamento e verificarne la compatibilità con il Regolamento.

Per quel che concerne i contenuti, l'articolo 30 prevede che nel registro siano annotate una serie di informazioni: in particolare, deve essere specificato il nome ed i dati di contatto del titolare del trattamento e ove previsto del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.

Vanno specificate le finalità del trattamento e descritte le categorie di interessati e dei dati personali trattati, nonché, le categorie di destinatari a cui dati sono stati o saranno comunicati, compresi i destinatari di paesi terzi o le organizzazioni internazionali. Se vi è un trasferimento di dati verso un paese terzo o un'organizzazione internazionale deve esserle data indicazione nel predetto registro compresa l'identificazione del paese terzo o l'organizzazione internazionale verso cui il dato viene trasmesso. Naturalmente, si dovrà dare atto nel medesimo registro di aver adottato garanzie adeguate, suffragando le attività con idonea documentazione; infine, dovranno essere indicati, laddove sia possibile, i termini previsti per la cancellazione dei dati e una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

La tenuta del registro non costituisce un adempimento formale, ma al contrario esso costituisce parte integrante di un sistema di corretta gestione del dato personale, pertanto, i titolari del trattamento ed i responsabili, a prescindere dalle dimensioni dell'organizzazione, devono compiere i passi necessari per dotarsi di

tale registro ed, in ogni caso, occorre compiere un'accurata ricognizione dei trattamenti per verificarne la compatibilità con il Regolamento.

7. Seppur succintamente, appare corretto sottolineare il disposto di cui all'articolo 32 relativo alle misure di sicurezza, dove, la normativa offre ai titolari del trattamento una serie di indicazioni che, sul piano tecnico, consentano l'ottimizzazione dei sistemi di gestione e la più efficace tutela dei diritti dell'interessato.

In particolare, la normativa incoraggia la **pseudonimizzazione** e la **cifratura dei dati** personali, attraverso sistemi che assicurino, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

Il sistema adottato dovrà, altresì, rispondere ad un'esigenza fondamentale ovvero quello di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico, ovvero, adottare tutte le cautele necessarie in caso di attacco informatico onde consentire di limitare i danni da aggressioni non previste e non prevedibili.

Chiaramente, l'adozione di un sistema di sicurezza idoneo non può prescindere dalla necessità di testare e verificare periodicamente l'efficacia delle misure di sicurezza tecniche ed organizzative adottate, pertanto, deve essere prevista una procedura di verifica che consenta di monitorare il corretto andamento del sistema così come ipotizzato e realizzato dal titolare del trattamento.

Anche i sistemi di sicurezza più performanti possono, però, subire aggressioni che mettono a rischio i dati, pertanto i titolari del trattamento – non solo i fornitori di servizi di comunicazione elettronica accessibili al pubblico – dovranno notificare al Garante per la protezione dei dati personali le violazioni di dati personali di cui vengono a conoscenza entro 72 ore dall'avvenuta intrusione ed, in ogni caso, darne notizia senza ingiustificato ritardo, laddove, ritengano che tali violazioni possano determinare rischi per i diritti e le libertà degli interessati.

La notifica all'Autorità, quindi, non è automatica, né obbligatoria essendo, ancora una volta, subordinata alla valutazione del rischio per gli interessati compiuta dal titolare, ma, anche in questo caso, la valutazione dovrà essere particolarmente prudenziale, onde, evitare che il titolare del trattamento, ovvero il suo

responsabile, possano incorrere nelle responsabilità declinate dal Regolamento a diverso titolo.

Il titolare del trattamento, in ogni caso, dovrà preoccuparsi di documentare le violazioni dei dati personali subite, anche se non ne ha data comunicazione all'Autorità di controllo e non abbia ritenuto necessario allertare gli interessati. Analogamente, per le violazioni subite, dovrà darsi conto delle circostanze, delle conseguenze e dei provvedimenti che, all'esito, il titolare del trattamento ha adottato. La documentazione di tali episodi risulta essere elemento protettivo indefettibile per il titolare del trattamento il quale, su richiesta del Garante, in caso di accertamenti, dovrà dare conto del l'*iter* seguito nella gestione dell'episodio e delle misure *self - cleaning* adottate.

8. Il completamento naturale del nuovo impianto normativo, potremmo dire, si sintetizza nella previsione di un responsabile della protezione dei dati, meglio noto come *Data Protection Officer* (DPO). Si tratta di una nuova figura professionale che il Regolamento prevede sia adottata obbligatoriamente per alcune categorie di soggetti e con riferimento a talune tipologie di trattamento.

Compito precipuo del DPO è la sensibilizzazione e la formazione del personale, nonché, la sorveglianza sullo svolgimento della valutazione di impatto del trattamento, secondo quanto previsto dall'articolo 35 del Regolamento.

Si tratta di una figura professionale che si caratterizza per indipendenza, autorevolezza e competenze manageriali. In particolare, l'articolo 37 ne prevede la nomina in tre casi specifici: a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico; b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; c) se le attività principali del titolare o del responsabile e consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati. La novità di tale figura professionale e la mancanza, allo stato, nel nostro sistema giuridico di prescrizioni qualificanti che si auspica provengano dal Garante per la protezione dei dati personali in tempi rapidi, consente di avere come unico riferimento le linee guida adottate dal Gruppo di lavoro ex art. 29 cui si rinvia per gli opportuni approfondimenti, in questa sede, val la pena sottolineare che, a prescindere dalla

nomina di un DPO, è fortemente raccomandato ai titolari ed ai responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se, nel caso specifico, sia o meno d'obbligo provvedere alla nomina di un DPO, in modo da dare atto che la *risk analysis* ha preso in esatta considerazione i fattori pertinenti. Se si procede alla nomina di un DPO su base volontaria, naturalmente, varranno per il medesimo le stesse prescrizioni previste per il caso di nomina obbligatoria.

Le conoscenze e le competenze del DPO consistono, prevalentemente, nella conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché, nella capacità di assolvere ai compiti al medesimo assegnati dall'articolo 39 del Regolamento: se nominato devono essere messi a disposizione degli interessati anche i riferimenti, ovvero, i dati di contatto del DPO.

Questa figura professionale risulta essere preziosa per il titolare non solo quando l'attività sia già avviata, ma, anche e soprattutto, nelle fasi iniziali in merito alla valutazione dei rischi atteso che uno dei compiti del DPO è proprio quello di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché, agli incaricati al trattamento che lo eseguono.

9. Queste, in estrema sintesi, le linee guida del nuovo Regolamento che impongono a chiunque effettui un trattamento di provvedere ai necessari adeguamenti. Tale obbligo prescinde, se non per le specificità evidenziate, dalle dimensioni dell'impresa ed impone a tutti i titolari l'adeguamento, stante il superamento, *in parte qua*, di quanto previsto dal Codice della Privacy, soprattutto, in vista dell'aggravamento del sistema delle responsabilità in capo al titolare e dell'imponente sistema sanzionatorio connesso.

10. In sintesi le **imprese** che operano a diversi livelli devono adoperarsi per un trattamento dei dati sicuro, adottando le misure tecniche e organizzative necessarie a garantire un approccio sereno al trattamento dei dati avendo cura di aumentare i livelli di sicurezza in proporzione alla rischiosità del trattamento effettuato e per la specificità delle attività poste in essere.

Devono essere in particolare, attenzionate le attività di *marketing online* che costituiscono certamente attività a rischio per la tutela dell'interessato e necessitano di interventi sotto il profilo, non solo della sicurezza del trattamento,

ma anche e soprattutto, della revisione della documentazione predisposta per l'acquisizione del consenso, ovvero, un'idonea informativa anche attraverso procedure, cosiddette stratificate, che consentono di isolare diversi trattamenti e di ottenere un consenso mirato. I mesi successivi all'implementazione definitiva del Regolamento saranno particolarmente intensi per il Garante che dovrà farsi carico, in linea anche con quanto sarà adottato dalla Commissione a livello europeo di individuare delle linee guida che non abbiano come obiettivo l'impinguamento di una sterile attività sanzionatoria, ma offrano spunti originali in grado di costruire il nuovo sistema di *accountability* nel rispetto delle reciproche attività e dei diritti dell'interessato.