Giovedi' 25/01/2018

Privacy - Regolamento UE - Studio di Commercialista

A cura di: Studio Valter Franco

Uno dei principi ribaditi più volte dal Garante e anche dall'art. 7 del Regolamento relativamente al consenso, e' che tutto sia facilmente comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'intendimento e' quindi quello di affrontare l'argomento utilizzando, appunto, un linguaggio semplice e chiaro, tanto per intenderci il linguaggio opposto a quello del legislatore, specie quello utilizzato in materia fiscale.

Si ritiene utile rammentare che il rispetto delle norme in materia di trattamento di dati personali è richiamatonelle convenzioniin essere tra lo studio e l'AgenziadelleEntrate (utilizzo di Entratel, cassetto fiscaleetc. etc.) ed il mancato assolvimento degli obblighiprivacy può causare spiacevoli effetti collaterali su tali convenzioni.

Il caro e vecchio "DPS" (documento programmatico sulla sicurezza) era stato abolito, ma ciò non esonerava il titolare del trattamento (cioè di norma il titolare dello studio) a dimostrare di aver posto in essere tutte le altre misure di sicurezza previste dal D.lgs. 196/2003 e dai relativi allegati (ed erano "misure minime" di sicurezza, un po' come dire "hai messo la porta blindata ma magarii ladri passano dalla finestra, forse è meglio che per evitare i furti installi anche un impianto di allarme"), così come ora, con il regolamento, occorrerà effettuare una valutazione del rischio, qualora ciò siastato omesso in precedenza e/o ne siano stati omessi gli aggiornamenti: sia in ambito antiriciclaggio che in ambito privacy, ma non solo, anche nel campo della sicurezza sul lavoro, il primo passo da compiere è quello della valutazione del rischio, dalla quale derivano poi le analisi sulle"protezioni" adottate e quelle da adottare. In effetti il Regolamento prevede che quando un tipo di trattamento preveda l'uso di nuove tecnologie e, considerato un rischio elevato peri diritti e la libertà delle persone, primadi procedere al trattamento venga effettuata una "Valutazione di impatto sulla protezione dei dati".

Ilregolamento UE 2016/679entrerà in vigore il 25 maggio 2018 e, sinceramente, non sono riuscito-probabilmente, anzi sicuramente, per incapacità - a rilevare cambiamenti sostanziali nell'assolvimento degli obblighi da parte di un 'normale' studio di commercialista.
Ovviamente il regolamento non si applica a trattamenti effettuati da una persona fisica per esercizio di attività a carattere esclusivamente personale o domestico (art. 1 c. 2 lett. c).

Una delle novità riguarda il Registro dei Trattamenti (art. 30) ma gli obblighi in materia non si applicano alle imprese od organizzazioni con meno di 250 dipendenti, quindi nessuna complicazione almeno per obbligo (poi il Garante consiglia l'adozione di tale registro in via "generale").Si segnala che il Garante Francese ha pubblicato sul proprio sito un modello di registro dei trattamenti in formato excel.

Altra novità (punti28-29 del considerando e art. 4 punto 5) riguarda la previsione, ai fini della protezione dei dati, di utilizzare la pseudonimizzazione, cosa che si ritiene irrealizzabile nell'ambito dello studio.
Le associazioni o organizzazioni rappresentanti categorie di titolari di trattamento possonoelaborare dei Codici di condotta (punto 98 del considerando e art. 40) in modo da facilitare i propri aderenti ad assolvere gli obblighi, specie per le micro-piccole e medie imprese (sul fac simile di quanto previsto in materia di antiriciclaggio).

Una delle conferme (punto 14 del considerando e art. 1) e' quella che la protezione prevista dal regolamento si applica alle persone fisiche, restando così esclusi dall'applicazione della norma i dati delle persone giuridiche e delle imprese dotate di personalità giuridica, osservando che nell'esecuzione di pratiche, ad esempio di una srl, vengono comunque trattati dati di persone fisiche (variazione di amministratori, variazioni di indirizzo di soci etc.), inoltre il regolamento non si applica ai dati delle persone decedute (punto 27 del considerando);per quanto riguarda il trattamento di dati dei minori l'articolo 8 fa riferimento ai minori di 16 anni (limitedi età recepito in Italia), aggiungendo che gli Stati membri possono stabilire anche un'età inferiore ma non ai 13 anni.

Dal regolamento europeo sembrava poi sparita la figura dell'incaricato del trattamento, mentre è riscontrabile nel punto 29 del considerando ('il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento') e nell'art. 4 punto 10 che indica espressamente che quale "terzo" debba anche intendersi "il responsabiledel trattamento e lepersone autorizzate al trattamento dei dati personali sotto l'autorità direttadel titolare o del responsabile".

Viene invece inserita la figura del Data Protection Officer (DPO), in pratica il "Consulente - Responsabile Privacy", in possesso di appositi requisiti professionali sia in materia di privacy che disicurezza informatica, la cui nomina è obbligatoria quando:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

L' ANSA ha pubblicato il 7 novembre 2017 una notizia nella quale viene stimato che in Italia dovranno essere impiegati più di 45.000 DPO e ciò, se da un lato può rallegrare in termini di incrementodell'occupazione, dall'altro comporta maggiori oneri per la pubblica amministrazione, oneri che vengono sopportati grazie all'imposizione diretta ed indiretta, mentre aziende e società si troveranno a sopportare maggiori costi.

Si consiglia, come è consigliabile farlo per l'antiriciclaggio, diaprire una cartella nella quale inserire i filesdi documentazione relativi alle norme in materia ditrattamento dei dati personali ed inizialmente si suggerisce di inserirein talecartellaIl testo del regolamento europeo e le guide del garante in materia.

Per le aziendelaMicrosoft ha attivato un sitoper l'autoverifica di quanto le procedre dell'azienda siano al momento conformi alle disposizioni delGDPR (General Data Protection Regulation) raggiungibile utilizzando il seguente link https://www.gdprbenchmark.com/it/questions precisando che taleautovalutazione non riguardale micro aziende.

Rag. Valter Franco

Fonte: http://www.studiofranco.eu