filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

# GDPR e PMI: breve manuale di sopravvivenza al nuovo regolamento privacy europeo

01 Febbraio 2018
ELSA, Margherita Trombetti

Sempre più vicini alla fatidica data del **25 maggio 2018**, giorno a partire dal quale le sue norme diventeranno definitivamente applicabili in tutti gli Stati membri dell'Unione europea, anche per le start up incombe il dovere di conformarsi alle previsioni del **nuovo Regolamento Privacy europeo: il GDPR.**
Il nome stesso è allo stesso tempo estremamente accurato e piuttosto fuorviante: General Data Protection Regulation, Regolamento Generale per la Protezione dei Dati.
Il motivo per il quale potremmo ritenerlo fuorviante è che il termine "regolamento" richiama subito l'ambito legale, relegandolo apparentemente a una prerogativa esclusiva degli "azzeccagarbugli" di turno, mentre il riferimento alla protezione dei dati suggerisce immediatamente una competenza esclusiva di coloro che si occupano di IT, lasciando "incolumi" tutti gli altri settori.
Niente di più sbagliato, invece: per assicurare una totale compliance, la risposta deve essere sistemica, deve provenire contemporaneamente da tutte le aree della realtà imprenditoriale che tratta dati personali.
Ma come e perchè si è arrivati a questo nuovo regolamento?

**Dalla direttiva al regolamento europeo**
La precedente normativa (ancora in vigore, almeno fino al 25 maggio), faceva riferimento alla direttiva europea 95/46/CE.
Prima di tutto questo atto normativo, datato 1995, era stato adottato prima della macroscopica diffusione di Internet, prima della nascita dei social network, prima dell'era della raccolta di dati su larga scala e della *digital economy*. Prima, quindi, che si sviluppasse questa concezione "invasiva" della tecnologia, diventata caratteristica peculiare dell'era digitale.
In secondo luogo, la natura stessa della **direttiva** la rende vincolante solo per quegli Stati dell'Unione europea che hanno previsto un atto di recepimento, presupponendo quindi l'adozione, da parte di ciascuna nazione interessata, di leggi interne che consentano di conformarsi alle misure e agli obiettivi previsti dalla direttiva stessa. Di fatto, questo può comportare la presenza, all'interno dell'Unione, di tante diverse interpretazioni quanti sono gli Stati che hanno recepito la direttiva: il risultato è un panorama perlopiù caotico e ostile per le realtà di business, dal momento che ogni impresa deve soffermarsi a valutare cosa può o non può fare in ciascuno degli Stati membri.

È per questo che l'intento principale del legislatore europeo, in fase di approvazione del GDPR è stato quello di prevedere delle regole che fossero unitarie e business-friendly, idonee a incentivare l'integrazione di quello che viene chiamato Digital Single Market. Le caratteristiche del regolamento infatti, a differenza di quelle della direttiva, ne consentono l'applicazione diretta in tutti gli Stati membri dell'Unione (senza rendere necessaria alcuna legislazione di attuazione) permettendo così la **creazione di un unico regime di protezione dei dati, comune a tutto il territorio dell'UE.**

Un altro significativo vantaggio portato dall'introduzione del nuovo regolamento è l'applicabilità nei confronti di tutti i soggetti che svolgono affari sul suolo europeo, anche di quelli che hanno ufficialmente sede fuori dall'Unione. Questo pone ufficialmente fine alla "discriminazione" fino ad ora sofferta dalle imprese basate nel territorio dell'UE, che **non subiranno più lo svantaggio** (dovuto proprio alla vecchia direttiva) di dover seguire regole relative alla protezione dei dati che invece non interessavano le concorrenti extra-europee.

**Oltre l'ambito di applicazione**

L'ultima novità, meno tecnica ma altrettanto rilevante, soprattutto quando si parla di nuove imprese innovative, è il fatto che il GDPR favorisce la creazione di un rapporto di fiducia tra realtà tecnologiche e imprenditoriali e consumatori. L'introduzione di regole nuove e decisamente più restrittive delle precedenti implica l'attribuzione di ruolo di "custode" a quelle realtà che si occupano di raccolta dei dati relativi agli utenti, arricchendo così un rapporto che prima veniva creato sulla base del mero interesse economico e allontanando l'aura di sospetto e ambiguità che troppo spesso caratterizza le relazioni B2C (*Business to Consumer*).

Si tratta quindi di regole che, se da un lato comportano senz'altro uno sforzo per assicurare la totale conformità del proprio modello di business e delle sue implicazioni pratiche, dall'altro rappresentano certamente un importante incentivo e un valore aggiunto per le aziende che dimostrano di "essere in regola". Per loro, il GDPR può diventare la chiave per il successo.

Ma in cosa consiste, nella pratica, lo sforzo che deve compiere un'impresa innovativa per assicurarsi la totale compliance, e quali sono le principali norme che interessano le start up?

**Nella pratica**

Al considerando n. 7, proprio nella prima parte del testo del nuovo Regolamento, si legge "**è opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata** tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche". Sono forse le parole che più di tutte rappresentano il **"nocciolo duro" del GDPR**, ma quale tipo di comportamento deve discendere da questi principi?

**1. Conosci il tuo business**

Quali dati raccogli? Quali sono le loro caratteristiche e in quali contesti vengono conservati e utilizzati? Gran parte della rivoluzione del GDPR consiste in una **forte *responsabilizzazione* del titolare del trattamento** (vedi al punto 2, "Accountability"), che deve operare la raccolta in modo **lecito, corretto e soprattutto trasparente.**

Uno strumento utile ad incentivare il rispetto delle finalità e dei parametri del regolamento è sicuramente quello del **registro delle attività di trattamento.** Si tratta di un documento in cui il titolare deve tenere traccia dettagliata delle attività compiute con dati relativi a dipendenti, fornitori, partner e soprattutto clienti (indicando in particolare le finalità del trattamento, le categorie dei dati e degli interessati, gli eventuali

trasferimenti verso paesi terzi dei dati raccolti e le misure di sicurezza adottate).

Quello della tenuta del registro è un **obbligo che non si applica alle imprese e organizzazioni con meno di 250 dipendenti,** a meno che il trattamento non sia occasionale o ad alto rischio, o includa particolari categorie di dati (ad esempio i dati sensibili). Tuttavia, esso può rappresentare anche per le piccole realtà una **risorsa per consentire una gestione più efficace e ordinata della sicurezza dei dati e dell'organizzazione**.

**2. Il principio di accountability**

In base al principio di ***accountability*** introdotto dal GDPR (tradotto in italiano con il termine "responsabilizzazione"), i titolari del trattamento devono **mettere in atto tutte le misure tecniche e organizzative necessarie** per assicurare, ed essere in grado di dimostrare, che la raccolta e l'utilizzo dei dati siano conformi alle nuove regole.

Il Regolamento non fornisce indicazioni precise su quali siano le misure pratiche da adottare: **l'approccio dovrà essere valutato caso per caso, tenendo in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento.**

A integrare questo approccio basato sulla valutazione del rischio intervengono i principi di ***privacy by design*** **e** ***privacy by default***. Si tratta di due concetti innovativi che impongono l'adozione di misure di protezione **fin dalla fase di progettazione del trattamento**, oltre a prescrivere un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Soprattutto in questo scenario di generale incertezza sulle misure pratiche da adottare, le *best practices* del titolare del trattamento rimangono quelle fondate su un **approccio integrato che interessi tutte le aree dell'azienda** (anche nel caso della start up), con una gestione interna ben strutturata che promuova la **cultura della privacy e della sicurezza dei dati personali.**

**3. La valutazione d'impatto**

Il **DPIA (Data Protection Impact Assessment)** è forse l'operazione più importante da effettuare per rispondere al principio di accountability. La valutazione del rischio conseguente a un ipotetico *data breach* rappresenta un **elemento fondamentale per la corretta gestione di tutto il ciclo del trattamento**, fin dalla predisposizione dei mezzi utili al trattamento stesso.

Per questo, in particolari casi quali la sorveglianza sistematica su larga scala, il trattamento di particolari tipologie di dati o nel caso di profilazione ad alto rischio, il Regolamento prescrive **una valutazione preventiva e sistematica delle finalità e della necessità del trattamento.** In relazione a questa vanno indicate tutte le misure e le garanzie previste per una adeguata protezione dei dati personali trattati.

Qual è la natura dei dati che potrebbero essere violati? I dati erano cifrati? **Con quanta facilità potrebbero essere identificati gli interessati?** Quanto gravi potrebbero essere i danni fisici, materiali o immateriali causati agli individui a cui i dati violati si riferivano? A tutte queste domande è necessario rispondere, anche sulla base delle **linee guida fornite dal Gruppo di lavoro ex art. 29.**

**http://ec.europa.eu/newsroom/document.cfm?doc_id=47711**

**4. In caso di data breach**

Se l'esame delle possibili fonti di rischio non è stato sufficiente ad evitare il verificarsi di una violazione dei dati personali, **il titolare del trattamento ha il dovere di comunicare la violazione all'autorità di controllo** (il Garante della privacy nazionale) entro 72 ore dal momento in cui ne è venuto a conoscenza.

Nel caso in cui la stessa violazione costituisca un **pericolo per le libertà e i diritti degli interessati**, anche ad essi dovrà essere fornita adeguata comunicazione.

**5. Bilanciamento degli interessi: le insidie per il direct marketing**

Si sa, **nell'era della digitalizzazione e dell'Internet of Things** i dati significano risorse e profitti. Ancora di più per le start up ad alto contenuto tecnologico, per le quali possono rappresentare non solo una **moneta di scambio, ma soprattutto una fonte di potere contrattuale**.

Con queste premesse potrebbe essere facile cadere nella tentazione di abusare di questo incredibile vantaggio: monitoraggio e profilazione forniscono una **maggiore conoscenza della propria clientela, favoriscono un *targeting* più efficace e una migliore pianificazione del proprio business**.

Il GDPR ha fatto un ulteriore passo avanti in favore delle aziende, stabilendo una volta per tutte che **l'interesse legittimo del titolare (anche quello per finalità di marketing diretto) *può* costituire una base giuridica sufficiente per consentire il trattamento.** Ciò significa che una prevalenza del legittimo interesse del titolare, che tra l'altro potrà essere valutata autonomamente dal titolare stesso, sarà **in grado di escludere la necessità di richiedere un esplicito consenso all'interessato**.

Ma non è tutto oro quello che luccica. Non soltanto il Regolamento compensa questo vantaggio con una serie di limitazioni (in particolare il **principio di minimizzazione**) che di fatto obbligano il titolare ad utilizzare la minor quantità di dati e il minor periodo di tempo possibili per le finalità del trattamento, ma **amplia anche il ventaglio di diritti dell'interessato**.

Il GDPR mette qualunque persona fisica nella condizione di compiere un consapevole esercizio dei poteri di controllo sui propri dati, garantendogli il **diritto all'informazione**, il **diritto all'accesso, alla rettifica e alla cancellazione** dei dati che lo riguardano, il **diritto alla limitazione del trattamento** e il **diritto di opposizione**.

Una novità assoluta è poi rappresentata dal **diritto alla portabilità dei dati**, che consente all'interessato di richiedere al titolare i propri dati in **formato strutturato** e leggibile da un elaboratore automatico, così da poterli **trasferire da un servizio ad un altro**.

Anche qui si tratterà quindi di effettuare una valutazione caso per caso, basata sul prudente **bilanciamento degli interessi del titolare e dell'interessato.** È ragionevole prevedere che nella maggior parte dei casi si dovrà ricorrere ad un **consenso** aggiornato e conforme a quanto previsto dalla nuova normativa, e dunque **inequivocabile** (esplicito solo nel caso di dati sensibili), **libero, specifico, informato, verificabile e revocabile.**

Lo scenario può risultare più complesso e le sanzioni per chi non si adegua saranno senz'altro pesanti (fino a 20 milioni o al 4% del fatturato mondiale annuo, se superiore), ma è tutto finalizzato a **incentivare il vantaggio competitivo delle aziende e la creazione di un mercato digitale europeo uniforme.**

Il 25 maggio si avvicina e anche alle nuove imprese innovative conviene accogliere con consapevolezza il cambiamento, per non essere lasciate indietro quando si trovano ancora alla casella "start".

***TAG:*** *accountability, GDPR, PMI, Diritto commerciale, Diritto della privacy, Diritto delle nuove tecnologie e delle comunicazioni*