Europartners Srl
P.IVA 07920511008
www.europartnersnetwork.eu
E-Mail info@europartnersnetwork.eu

GDPR: Regolamento generale sulla protezione dei dati personali

Impatti economici e sociali sul mercato nazionale[1]

Key Messages

Responsabilizzazione. La scelta delle misure di sicurezza viene demandata al "Titolare"

Le imprese saranno obbligate ad operare valutazioni di impatto, con relative misure di sicurezza. DPIA

DEEP per la valutazione degli impatti e valutazione del costo aziendale per adeguamento al GDPR

Premessa. Significato di GDPR

Il 25 maggio 2018 sarà applicabile in via definitiva, in tutti gli stati membri dell'Unione Europea, il nuovo Regolamento generale sulla protezione dei dati personali, cosiddetto GDPR.

Il Regolamento generale sulla protezione dei dati ha come scopo principale quello di uniformare il processo relativo alla protezione dei dati a livello europeo, superando così le normative nazionali, talvolta differenti tra loro nel recepimento della Direttiva 95/46UE, oggi abrogata.

Ma quali sono le novità? A che cosa devono fare attenzione le aziende e i gestori di siti web? Quanto costerà alle aziende l'adeguamento al GDPR? E quale sarà lo scenario probabile dopo la data fatidica del 25 maggio 2018?

Dall'entrata in vigore, tutte le aziende e tutte le istituzioni pubbliche che lavorano con i dati di privati, compresi quelli dei dipendenti, sono tenute a rispettare la nuova regolamentazione europea sulla protezione dei dati. La questione della tutela della privacy coinvolge un numero enorme di tipologie aziendali. Oltre agli enti che sfruttano i dati per fini di marketing, i motori di ricerca e i social network, il cui business è retto sui big data, dovranno attenersi ai principi del GDPR anche le aziende sanitarie ed energetiche, le banche, ma anche i centri estetici.

[1] Di **Prof. Avv. Sabina Bulgarelli** (Diritto dei Media e dei Dati Personali, Università Telematica Internazionale UNINETTUNO) – **Olivier La Rocca** (Presidente CdA Europartners – o.larocca@europartnersnetwork.eu)

Potenzialmente, qualsiasi impresa potrebbe dover fare i conti con le direttive imposte dall'Unione Europea.

Un altro aspetto importante riguarda la portata semantica del concetto di "dato personale": in esso si ricomprende non solo un nome o un indirizzo di posta elettronica, ma anche una foto, un indirizzo IP, una geolocalizzazione. A più di vent'anni dall'entrata in vigore della prima legge sulla privacy, in Italia, si pensa ancora che per dato personale debba intendersi il nome e il cognome, la data di nascita e il codice fiscale di una persona e non si considera che anche una semplice busta-paga è in grado di rivelare dati ben più "sensibili", come l'appartenenza ad un sindacato. La maggior parte delle aziende non è a conoscenza dell'urgenza relativa al rispetto del RGPD e soprattutto della sua portata pervasiva.

Secondo un rapporto pubblicato a settembre 2017 dall'Osservatorio Information Security & Privacy del Politecnico di Milano, solo il 27% delle aziende è a conoscenza degli obblighi del regolamento e solo il 9% ha avviato un progetto concreto per l'adeguamento. Per il 23% del campione, non vi è alcuna consapevolezza di quelle che sono le implicazioni, soprattutto, e questo è il dato più allarmante, per quanto riguarda le sanzioni previste, che arrivano sino ad € 20.000.000,00 o fino al 4% del fatturato mondiale annuo. La metà dei soggetti interessati sta ancora svolgendo un'analisi dei requisiti richiesti e dei piani di attuazione possibili, ma solo nel 9% è già in corso un progetto strutturato di adeguamento alla normativa. Solo il 7% delle organizzazioni ha accantonato un budget dedicato.

Ma quanto costerà ad un'azienda adeguarsi al GDPR?

Il 75% delle multinazionali Europee ha previsto un investimento di almeno 5 milioni di euro per l'adeguamento al GDPR, con l'assunzione di almeno 2 o 3 dipendenti dedicati a tempo pieno alle questioni relative alla privacy. **Si stima che più del 78% delle aziende italiane non risulterà in regola con l'adeguamento al GPDR entro maggio 2018.**

Questo dato è il risultato, dai dati in nostro possesso da un approccio minimalista, alimentato dal proliferarsi di soluzioni low cost, spesso software elaborati ad hoc, che danno l'illusione di "essere in regola" con il GDPR. Nel contesto italiano, questo tipo di soluzioni viene adottato in larga parte dalle PMI, che nel 2016 avevano raggiunto quota 145.000, considerato che il budget dedicato è spesso molto esiguo. Ma se l'informativa all'interessato, il consenso e le figure della privacy, salvo il Data Protection Officer, già si conoscevano, perché previsti dal Codice della Privacy, a mettere in crisi i soggetti destinatari degli obblighi previsti dal GDPR, è soprattutto l'attuazione del principio di accountability.

L'art. 5 del RGDP individua nel Titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento dei dati personali, quali quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza.

Il Titolare, oltre a dover garantire il rispetto dei suddetti principi, deve essere in grado di "comprovarlo", in quanto tale soggetto ha l'onere di porre in essere una serie di adempimenti e di elaborare le misure di sicurezza adeguate, che rendano i principi posti dalla nuova disciplina dati verificabili nei fatti e non più soltanto obblighi giuridici astratti.

Il concetto di "Responsabilizzazione" viene ulteriormente delineato dall'art. 24 del Regolamento, il quale prevede che il Titolare del trattamento debba mettere in atto adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina. In buona sostanza, la scelta delle misure di sicurezza viene demandata al Titolare, che deve valutare di volta in volta, quali sono le più adeguate in relazione ad una serie di elementi tra cui la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

La nuova disciplina non prevede più una serie tassativa di "misure minime" che è necessario adottare, ma lascia l'onere della scelta in capo al Titolare. Se la scelta si rivelerà sbagliata, verranno applicate le pesanti sanzioni.

Da un lato, il RGDP lascia maggiore discrezionalità al Titolare del trattamento nel decidere attraverso quali modalità tutelare i dati, dall'altro, tuttavia, riversa un gravoso onere in capo allo stesso, che si trova a dover dimostrare le motivazioni che hanno portato all'adozione di una determinata decisione, oltre che documentare le scelte effettuate.

In linea con tale principio, che in altri termini impone una responsabilizzazione del Titolare del trattamento dei dati, si introduce l'obbligo di effettuare una Valutazione di impatto sulla protezione dei dati (DPIA o Data Protection Impact Assessment). Le aziende pubbliche e private sono obbligate ad operare una valutazione di impatto, stabilendo quali misure di sicurezza adottare così da ridurre il rischio. Questo adeguamento è particolarmente importante per le aziende che si occupano di Cloud Computing, e che quindi maneggiano grandi quantità di dati di persone. Ancora più nello specifico, questa modifica riguarda la aziende che archiviano dati sanitari, i quali essendo particolarmente sensibili, aumentano considerevolmente la gravità nel caso in cui vengano diffusi.

Scenari possibili dopo il 25 maggio 2018

Molte imprese per evitare rischi potranno scegliere di esternalizzare la gestione dei dati. Altre investiranno di più sul social media marketing: dal momento che il motore di questi canali sono proprio i dati, è chiaro che i social network saranno le prime aziende a mettere al sicuro i propri sistemi per evitare sanzioni.

Il GDPR avrà per le aziende, soprattutto per quelle che investono capitali nelle nuove tecnologie che comportano monitoraggio sistematico di persone e che fanno profilazione, o quelle del settore sanitario, impatti organizzativi ed economici importanti.

Da questo punto di vista, i **Codici di Condotta e le certificazioni, previsti dagli artt. 40 e 41, costituiscono uno strumento fondamentale per tracciare un percorso più snello e meno oneroso, anche dal punto di vista economico**.

Dal momento che l'onere della prova viene posto in capo al Titolare e al Responsabile del trattamento, dovendo gli stessi essere in grado di dimostrare di aver messo in atto misure organizzative e di sicurezza adeguate alla particolare tipologia di dati che trattano e agli specifici trattamenti che effettuano, i Codici di Condotta e le Certificazioni si porranno come elementi di prova, o meglio come presunzioni di conformità al Regolamento. Molti "considerando" e molti articoli, infatti, stabiliscono che se il Titolare o il Responsabile aderiscono ad un Codice di Condotta, possono essere considerati conformi al Regolamento. Il Codice di Condotta è un documento redatto dalle associazioni e dalle organizzazioni che rappresentano categorie di titolari del trattamento o di responsabili del trattamento, aventi lo stesso profilo. I Codici di Condotta dovrebbero tenere conto delle caratteristiche specifiche dei settori di riferimento e delle diverse esigenze connesse alle dimensioni aziendali. Dovrebbero contenere norme di dettaglio e semplificazioni applicabili alle imprese consociate o aderenti.

Quindi, dopo la data fatidica del 25 maggio 2018, uno scenario possibile potrebbe essere rappresentato, oltre che dai Codici di Condotta da parte delle associazioni di categoria, anche dall'obbligatorietà di certificazioni privacy, quale presupposto per partecipare ai bandi di gara della Pubblica Amministrazione.

Ma nell'era dei Big Data, i veri centri d'interessi economici sono i colossi che gestiscono i dati personali a livello internazionale. Del resto, il regolamento si applicherà a chiunque nel mondo offrirà beni e servizi o profilerà cittadini europei, a prescindere dal fatto che abbia la propria sede o il server all'estero.

Le conseguenze economiche per i colossi del web non sono rappresentate solo dalle sanzioni amministrative previste dal regolamento, che possono arrivare sino al 4% del fatturato annuo mondiale, ma anche dalle ricadute delle quotazioni in borsa. Ed è ciò che sta accadendo a Facebook proprio in questi mesi.

Partendo da queste analisi, stiamo lavorando sull'analisi degli impatti territoriali con lo strumento DEEP.

Progetto valutazione dell'impatto economico e sociale – Report Novembre 2018

Il progetto è partito a Marzo 2018, con le rilevazioni puntuali sulla norma e le procedure attuate a livello comunitario e nazionale. Parte delle rilevazioni hanno evidenziato quanto definito brevemente nel presente paper.

La definizione dei parametri con le rilevazioni territoriali, saranno implementate con lo strumento DEEP. Si andrà a lavorare dal 25 maggio 2018 sino al 31 ottobre 2018, nei contesti territoriali a livello comunale per misurare la percezione (attraverso 2 waves di sentiment) e i dati strutturali. Le informazioni suddivise per tipo di importanza e gerarchizzate, misureranno l'impatto territoriale dell'adozione del regolamento sui territori. Offrendo spunti per leggere le eventuali criticità o anche buone prassi che verranno codificate.

In parallelo, attraverso l'utilizzo di metodi di matematica finanziaria, sarà misurato quello che al momento sono previsioni di costo per l'adeguamento aziendale. Il costo si suddividerà in varie tipologie, andando a prendere come riferimento il costo di adeguamento delle competenze delle risorse umane o di assunzione, o ancora di esternalizzazione ad altre società. Il costo per la codifica del codice di condotta e degli enti certificatori. Il costo di cambio di procedura e/o di creazione o acquisizione di sistemi informatici di protezione.

L'output è un report analitico che offrirà le seguenti informazioni:

- Impatto sul territorio, con visualizzazione territoriale e cruscotti interattivi degli scenari a livello comunale;
- Costi di adeguamento al GDPR, suddiviso per aree e territori sempre geovisualizzati.