# Nuovo GDPR, per Napoli e Knowles, regolamentazione non tassativa e ancora da decifrare nella sua interezza

**Date :** 10 luglio 2017

Nel corso dell'RSA Summit 2017 di Roma abbiamo incontrato Rashmi Knowles, Chief Security Architect EMEA, RSA e Giovanni Napoli, Enterprise EMEA security Architect Team Lead. Con loro abbiamo approfondito alcuni aspetti del nuovo GDPR, analizzando in particolar modo i lati più controversi di questo.

## Il GDPR aumenta la privacy per gli individui e dà alle autorità di regolamentazione maggiori poteri per agire contro le imprese che violano la nuova legge. Come risponderà l'Italia a queste nuove disposizioni?

**Napoli:** Questo nuovo regolamento riguarderà tutte le aziende che trattano dati personali. Anche in Italia c'è una forte attenzione all'argomento e, non a caso, una parte del nostro Summit è stata proprio dedicata al tema GDPR. In tanti – clienti e partner - si chiedono quali implicazioni avrà, in termini di compliance, azioni da prevedere, impatti legali, procedurali e organizzativi, l'entrata in vigore del GDPR.

Gli aspetti che sembrano preoccupare di più sono quelli legali: ci si chiede che tipo di ammende saranno previste e se entreranno in vigore immediatamente. Ma anche quali nuovi processi bisognerà mettere in atto per essere sicuri di poter rispettare il regolamento, quali professionalità saranno necessarie per gestire i nuovi processi e le tecnologie che dovranno essere implementate.

Il ruolo di RSA è quello di far comprendere che il GDPR riguarda principalmente la gestione del rischio, dal momento che, tra le altre cose, introduce l'obbligatorietà tempestiva – in 72 ore - di notifica di una breach. Le aziende devono quindi capire se hanno i mezzi, le tecnologie e i processi necessari per poter individuare e reagire in tempo reale a una violazione.

**Knowles:** Ci sono ancora degli aspetti poco chiari in questo regolamento, tanto che molte organizzazioni in tutta Europa lo stanno studiando per capire come attuarlo. Ad esempio, relativamente al tema delle ammende, non è ancora chiaro quale sarà la loro entità: se quella minima sarà del 2% o anche meno, e se, in caso di grave violazione, questa potrà arrivare al 4%.

Al momento, all’interno del regolamento vengono presentate delle best practice, ovvero indicazioni di come fare le cose, come proteggere i dati ecc.. E grazie al fatto che la sua adozione è imminente, molte organizzazioni, o almeno quelle più grandi, stanno prendendo coscienza che le norme imposte dal GDPR sono in realtà delle buone regole da adottare per proteggere il proprio business, un’occasione per mettere in atto una serie di processi che li metta nelle condizioni di accorgersi di aver subito un attacco (breach awareness) e affrontarlo.

**Napoli:** Il regolamento si basa sul fatto che ogni azienda dovrebbe conoscere i pericoli odierni in termini di cyber risk e attacchi alla sicurezza informatica e prendere coscienza che questa sfida implica nuove minacce.

Ancora non sappiamo se sarà così, ma ci aspettiamo che le autorità preposte facciano delle verifiche per controllare se le aziende hanno adottato delle procedure, se dispongono di una organizzazione adatta a individuare eventuali attacchi che tengono conto proprio dell’evoluzione delle minacce.

## Il DPO (Data Protection Officer) diventerà obbligatorio per le aziende che elaborano grandi volumi di dati personali. Quali rischi correrà il DPO se non saranno rispettate le norme?

**Knowles**: Il DPO avrà la responsabilità di assicurare che la gestione dei dati avvenga in sicurezza; dal nostro punto di osservazione, notiamo che tra le aziende vi è la consapevolezza che questo dovrà avere un livello di competenze molto elevato, perché dovrà farsi promotore del GDPR, assicurando il massimo allineamento tra coloro che processano i dati e coloro che li controllano. Non ne saranno responsabili in ultima analisi perché, secondo il regolamento, questa responsabilità riguarderà chi processa e chi controlla i dati, ma ovviamente il DPO dovrà monitorare l’applicazione del regolamento.

A mio avviso, un tema che emergerà presto – a livello europeo e globale – è la mancanza di DPO rispetto a quanti ne sarebbero necessari. Per fare un esempio, le commissioni nel Regno Unito hanno previsto che nel prossimo anno ne avranno bisogno di almeno 60mila.

## Può spiegarci l'importanza della gestione degli accessi quando si tratta di soddisfare il Principio del privilegio minimo previsto nel GDPR?

**Napoli** I due concetti sono collegati: la gestione degli accessi incide sulla gestione del rischio. Il fatto che oggi siamo in grado, all’interno di una azienda, di assicurarci che colui che accede ad una determinata risorsa sia effettivamente la persona autorizzata a farlo, permette di mitigare molti rischi.

Quest'anno, e fino ad ora, circa l'81% delle violazioni dei dati sono state causate dal fatto che le credenziali di accesso sono state rubate. Limitando all’utente i dati al quale è possibile accedere, si riduce di fatto la possibilità di danneggiare l’azienda.

**Knowles**: Questo è un tema molto interessante sul quale, allo stato attuale, il GDPR non dà

indicazioni chiare. Il fatto di dover consentire ai cittadini l'accesso ai propri dati, per verificarne la correttezza e aggiornarli, comporta che questi possano essere trasferiti e affidati a terzi.

Come si è ricordato, molte violazioni sono causate dal furto di credenziali. Il tema dell'Identity management e della sua governance è molto importante, ma nel regolamento non è affrontata.

## Alcuni obblighi e/o esenzioni sotto il GDPR derivano direttamente dal livello del rischio. Quali sono le diverse tecniche di mitigazione e la loro efficacia nel ridurre il rischio?

**Knowles:** Da un punto di vista tecnologico esistono diverse soluzioni. La più diffusa è la crittografia, ma sappiamo che non è necessariamente quella migliore poiché lascia ancora molte questioni aperte riguardo le violazioni.

Personalmente, penso che si debba agire più a livello di approccio, colmando le lacune esistenti nel processo di sicurezza. E in questo il GDPR darà un grande aiuto perché prevede che, se si è vittima di un incidente nella sicurezza, questo deve essere tempestivamente segnalato. Ciò può avvenire se si hanno strumenti idonei in grado di rilevare molto velocemente la violazione e gestirla adeguatamente. Ed è qui che notiamo le maggiori lacune.

Prima di tutto occorre che una azienda riduca al minimo il "dwell time": più i criminali rimangono nella tua rete, maggiori sono i danni che possono fare. Poi occorre sapere neutralizzare l'attacco, mitigandolo e applicando un programma ben preciso e predefinito di risposta agli incidenti.

RSA ha osservato che un terzo delle aziende non dispone di questo programma o, chi lo dispone, non lo ha mai utilizzato. Con l'entrata in vigore del GDPR questo non sarà più possibile: il GDPR infatti, al contrario ad esempio di compliance di tipo PCI-DSS, che prevede un esame semestrale e la possibilità di adeguare la propria formazione in base alle lacune evidenziate dal test, si basa su una implementazione continua e quotidiana, a prescindere dallo strumento utilizzato per rispettare la compliance.

**Napoli**: Concentrandoci su questo ultimo aspetto, il GDPR appare fondamentalmente un processo di governance, quindi significa che potrebbe bastare semplicemente un foglio Excel per gestire la valutazione dei rischi legata alla gestione dei dati, che è l'oggetto del GDPR. Sappiamo però che approcci manuali di questo tipo sono inefficaci ed onerosi. Per far fronte a queste necessità, RSA propone, oltre alle specifiche soluzioni di gestione delle violazioni e identity management, l'utilizzo di tecnologie GRC (Governance Risk & Compliance) che possono davvero guidare le aziende al rispetto del GDPR in modo graduale; non si tratta infatti di un processo immediato ma che prevede degli step.

**Knowles:** Il processo va automatizzato, utilizzando l'analisi in tempo reale dei dati. Solo così è possibile intervenire e avviare l'automazione; con le nostre soluzioni GRC, se si individua una vulnerabilità a causa di una violazione, questa viene immediatamente risolta e, automaticamente, il sistema si migliora.

## È necessario adottare precauzioni particolari quando i dati personali vengono trasferiti in paesi al di fuori della UE che non garantiscono una protezione dei dati standard. Cosa si può fare per salvaguardare la privacy?

**Knowles:** Il GDPR è un regolamento globale e prevede che tutti coloro che gestiscono dei dati lo debbano utilizzare. Dunque se una azienda trasferisce dati fuori dalla UE, come negli USA o in Sud America o ovunque, le organizzazioni che li elaborano dovranno rispettare il GDPR.

Dal punto di vista giuridico, il regolamento non spiega come questo accadrà, ma penso che ci siano tre possibilità: la prima è che la società che riceverà i dati sia in regola col GDPR; la seconda è che abbia una sorta di Privacy Shield, ma penso che questo approccio sia poco probabile; la terza è continuare a seguire quanto viene fatto oggi: stipulare un contratto ad hoc con la società che riceve i dati da elaborare.

## Ci sono altri aspetti del GDPR che meritano di essere analizzati?

**Napoli:** Maggio 2018 è davvero vicino: per mettere a punto il processo giusto, la tecnologia adeguata o almeno convalidare quella che già si possiede ci sarà bisogno di molto tempo. La mia raccomandazione è quella di muoversi quanto prima per sfruttare al massimo i – pochi – mesi che rimangono.

Rashmi Knowles, Chief Security Architect EMEA

Giovanni Napoli, Enterprise EMEA security Architect Team Lead

A cura della Redazione