AZIENDABANCA

Mensile

Data 05-2015
Pagina 34/35
Foglio 1 / 2

In banca arriverà il Privacy Officer

IL RESPONSABILE DELLA PROTEZIONE DEI DATI È UNA DELLE PRINCIPALI NOVITÀ DEL FUTURO REGOLAMENTO EUROPEO SULLA PRIVACY, ANCORA IN LAVORAZIONE. UN NUOVO RUOLO, INTERNO ALLA BANCA O IN OUTSOURCING, CHE DOVRÀ RISPETTARE LE GARANZIE DI AUTONOMIA PREVISTE DALLA CIRCOLARE 263 E DISPORRÀ ANCHE DI UN BUDGET PER VIGILARE SUL RISPETTO DELLE REGOLE SULLA PRIVACY

Il Regolamento europeo in materia di protezione dei dati personali è ancora in lavorazione. La versione definitiva del testo è attesa per la fine del 2015, se non addirittura per l'inizio del prossimo anno. Alcuni punti fermi della nuova normativa, comunque, sono già ben delineati: riguarderà di certo anche le banche, le assicurazioni e altri player del mondo finanziario l'obbligo di dotarsi di una nuova figura, il Responsabile per la Protezione dei Dati. «L'iter legislativo è ancora in corso – afferma Luca Spongano, Consigliere della Sezione Territoriale AICA dell'Emilia Romagna, membro del Gruppo Diritto ICT e Privacy e referente per le tematiche Privacy e sicurezza – ma certamente le banche saranno tra le aziende chiamate a individuare una nuova figura, quella del Data Protection Officer o del Privacy Officer. Un professionista che avrà il compito di supervisionare il trattamento dei dati in azienda, fornendo consigli e osservazioni per il rispetto della normativa in materia. L'ultima versione del testo votata dal Parlamento Europeo, risalente a marzo 2014, prevede l'obbligo di dotarsi di un Privacy Officer per le aziende pubbliche, per le aziende la cui attività principale riguarda il trattamento dei dati "sensibili" e per tutte le persone giuridiche che gestiscono i dati di almeno 5mila persone in 12 mesi consecutivi, compresi per esempio clienti e dipendenti».

Il Regolamento si somma alle misure esistenti

Per il settore bancario, il Regolamento europeo andrà a intersecarsi con il dettato della Circolare 263 di Banca d'Italia e con il provvedimento ad hoc che il Garante sulla Privacy ha emanato, nel 2011, per regolare la circolazione delle informazioni in ambito bancario. «Le misure già previste potrebbero essere sovrapponibili alle attività previste dal testo in discussione a livello europeo – spiega Spongano. Il Data Protection Officer, ad esempio, non dovrà presentare potenziali conflitti di interesse, in linea con quanto disposto dalla 263. Questa nuova figura non dovrà quindi dipendere dalle disposizioni aziendali: ci sono realtà in cui la privacy può

Luca Spongano, Consigliere della Sezione Territoriale AICA dell'Emilia Romagna, membro del Gruppo Diritto ICT e Privacy e referente per le tematiche Privacy e sicurezza

essere solamente ed impropriamente vista come un ostacolo al business, per questo è importante garantire l'indipendenza della funzione che sarà chiamata a garantire il rispetto della normativa. Anche perché il Regolamento specifica che l'azienda, cioè il Titolare del trattamento dei dati personali, dovrà dare disponibilità al proprio Data Protection Officer di mezzi, personale, locali: tutte le strutture necessarie per mantenere la propria autonomia professionale, compresi i poteri di spesa per consentire all'azienda di essere conforme, ad esempio con la frequenza di corsi di formazione».

Quando sarà obbligatorio dotarsene

Il Regolamento darà comunque due anni di tempo alle aziende per mettersi a norma: stiamo quindi parlando di misure che non scatteranno prima della fine del 2017. Il vero "nodo" da risolvere resta il criterio per cui in azienda la figura del Data Protection Officer sarà obbligatoria o semplicemente "consigliata". «In una precedente bozza, il Privacy Officer era obbligatorio nelle imprese con oltre 250 dipendenti – precisa Spongano – mentre in un secondo momento anziché alle dimensioni aziendali si è messo l'accento sul numero di soggetti i cui dati vengono trattati».

Quali competenze deve avere

Mentre è abbastanza chiaro che il Responsabile della Protezione dei Dati potrebbe essere «interno all'azienda, esterno oppure presente come un mix delle due tipologie – continua Spongano – con una funzione interna e un soggetto esterno la cui attività è regolata da un contratto di servizio. Il Regolamento specifica che si tratta di un incarico di durata prestabilita, almeno 4 anni se affidato in outsourcing, ovviamente con possibilità di rinnovo. Il Responsabile dovrà possedere una conoscenza specialistica della normativa ma anche una esperienza tale da garantire l'adempimento a ciò che prevede la normativa: il tutto calibrato in relazione alla tipologia dei trattamenti effettuati in azienda sui dati. In questa direzione va inteso lo strumento di apprendimento e di verifica realizzato da AICA con il Modulo di Certificazione "Protezione dei dati personali – Privacy e Sicurezza"».

> LE BANCHE DOVRANNO DOTARSI DI UNA NUOVA FIGURA: IL RESPONSABILE PER LA PROTEZIONE DEI DATI

Una guida agli adempimenti

Una sorta di Garante della Privacy interno e "in piccolo", che potrà trovarsi nella posizione scomoda di controllore e supervisore di tutto ciò che l'azienda fa utilizzando i dati di clienti e dipendenti. «Il nome del Responsabile della Protezione dei Dati dovrà essere comunicato all'autorità di controllo e agli interessati nell'informativa – aggiunge Spongano. Già oggi, e a maggior ragione dopo la pubblicazione del Regolamento, in caso di trattamento illecito il Titolare del trattamento deve dimostrare all'autorità giudiziaria di aver fatto tutto il necessario per evitare la violazione delle norme. Il Data Protection Officer avrà quindi il compito fondamentale di guidare all'adozione non solo degli adempimenti "obbligatori" ma anche di quelli "consigliabili"».

Una struttura indipendente per la privacy?

All'interno delle banche sono già presenti delle strutture che hanno tra le loro mansioni anche il compito di consentire alla banca di essere compliant alla normativa sulla privacy. «Questi "uffici privacy" sono realtà anche in molte grandi aziende, come le multiutility – conclude Spongano – ma indubbiamente sono in corso evoluzioni per adeguarsi alle linee generali del Regolamento. La stessa Circolare 263 di Banca d'Italia prevede funzioni di compliance e presidi specializzati separati: sarà interessante vedere se nel mondo bancario si creeranno delle strutture a se stanti dedicate esclusivamente al tema della privacy».

A.G.