Intervista al DPO del Gruppo Mediobanca, dott. Pierandrea Ginex

Gaetano Arnò
Avvocato cassazionista, già docente di Diritto industriale – Diritto dell'informatica presso l'Università Cattolica di Milano, Data Protection Officer Network PwC Italy

Privacy& ha incontrato il dott. Pierandrea Ginex, Data Protection Officer di Mediobanca e delle sue controllate italiane, con l'obiettivo di approfondire i principali aspetti di interesse, sotto il profilo della data protection, per uno dei principali gruppi bancari italiani.
Il dott. Ginex è entrato nel Gruppo Mediobanca nel 2003, dopo un'esperienza in Banca Nazionale del Lavoro, occupandosi dapprima di organizzazione e, successivamente, di conformità normativa, con crescenti responsabilità. Attualmente, oltre a ricoprire l'incarico di Data Protection Officer del Gruppo Mediobanca, è Direttore Centrale Compliance di Compass Banca. È infine Coordinatore della Commissione Giuridica di Assofin (Associazione Italiana del Credito al Consumo e Immobiliare).
Il dott. Ginex ha avuto il piacere di condividere con noi la sua esperienza da DPO, raccontandoci le sfide e le complessità del ruolo, assunto a ridosso dell'entrata in applicazione del GDPR.

Q: Benvenuto Dott. Pierandrea Ginex e grazie per aver accettato il nostro invito. Per iniziare vorremmo chiederle qualche informazione aggiuntiva in merito al Gruppo Mediobanca. Nell'immaginario comune, Mediobanca è una banca d'affari che nasce per supportare le imprese in operazioni complesse di espansione, internazionalizzazione e finan-

ziamento, tuttavia sappiamo che oggi il modello di business del Gruppo è fortemente distintivo. Quali sono, oggi, i principali settori di attività delle società del Gruppo?

Dott. P. Ginex: In 75 anni di storia, Mediobanca si è affermata come banca d'affari di riferimento in Italia, accompagnando la crescita e l'internazionalizzazione delle imprese italiane con un'offerta creditizia completa, qualità assoluta dei servizi, riservatezza e affidabilità. Fin dalla fondazione, il *corporate & investment banking* ha rappresentato l'asse portante dello sviluppo della banca, rendendola ancora oggi riconoscibile anche a livello internazionale. Tuttavia, negli anni, Mediobanca ha saputo ridisegnare il proprio profilo, avviando e consolidando un processo di trasformazione da banca d'affari e *holding* di partecipazioni a gruppo finanziario specializzato, maggiormente orientato alla profittabilità piuttosto che ai volumi.

In questo sentiero evolutivo, il Gruppo ha saputo collocarsi anche in segmenti di attività specialistici, quali il *consumer banking*, con la controllata Compass Banca, attiva principalmente nel finanziamento dei consumi delle famiglie, e il recupero crediti, *core business* di MBCredit Solutions, società che vanta un'approfondita conoscenza dei servizi di tutela, gestione e recupero delle posizioni insolute e che ha consolidato negli anni l'esperienza nell'acquisto e gestione di crediti non performanti. Il Gruppo è altresì presente nel comparto *leasing* con SelmaBipiemme, nel *factoring* con MB Facta e sta crescendo in modo importante nel w*ealth management*, attraverso un modello distintivo che si fonda sulla stretta sinergia con la divisione Corporate & Investment Banking del Gruppo. Nel *wealth management* rientrano Mediobanca Private Banking, CheBanca!, CMB Monaco oltre alle fabbriche prodotto (Mediobanca SGR, Cairn Capital e RAM AI).

Q: A questo punto, alla luce della elevata diversificazione del business, viene spontaneo chiederle quale sia la logica che il Gruppo ha deciso di adottare con riferimento alla data protection. Nello specifico, come è organizzata la struttura DPO e che tipo di competenze avete ritenuto necessarie per l'assolvimento dei compiti assegnati al DPO dal GDPR?

Dott. P. Ginex: Il Gruppo ha optato per un unico Data Protection Officer per le controllate italiane, ricorrendo a un modello accentrato con designazione di una risorsa interna per garantire un approccio omogeneo all'adeguamento alla normativa, nonché un'ottima conoscenza delle realtà aziendali di Gruppo. A supporto del DPO, è stata costituita una struttura composta da tre risorse, l'unità Group Data Protection, che offre consulenza alle società italiane del Gruppo e coordinamento alle società estere.

La scelta di una figura interna è stata dettata principalmente dall'elevato grado di diversificazione delle società del Gruppo, circostanza che avrebbe potuto creare qualche difficoltà – per lo meno iniziale – a un professionista esterno, mentre la previsione di un'unità organizzativa a riporto del DPO è motivata dall'esigenza di garantire al Responsabile della protezione dei dati un supporto operativo nel continuo.
La struttura DPO è stata organizzativamente inserita nell'ambito della Funzione Compliance della Capogruppo, posto che i compiti assegnati alla nuova figura apparivano assimilabili, nel contesto della regolamentazione bancaria, a quelli tipici di una funzione di controllo di secondo livello. Tale scelta ha inoltre agevolato la relazione con le funzioni di conformità delle singole *legal entities*, che rappresentano il naturale punto di contatto con il DPO nell'operatività quotidiana.
Il *team* DPO è caratterizzato, per precisa scelta di indirizzo, da competenze decisamente eterogenee, combinando profili di natura giuridica, organizzativa e di matrice IT. Abbiamo, in altri termini, ritenuto piuttosto improbabile individuare profili trasversali sui tre ambiti, optando quindi per la coesistenza di profili specialistici. Come tutte le scelte, anche questa ha determinato opportunità e rischi. Sul primo fronte, abbiamo la garanzia di poter affrontare distinte tematiche con un elevato grado di preparazione su ciascuna di esse. Di contro, è importante definire una sorta di linguaggio comune all'interno del *team* e garantire frequenti momenti di condivisione delle informazioni.
A tre anni dall'adozione del modello, ritengo che questa impostazione abbia dimostrato di essere decisamente solida in termini di valore apportato rispetto alle tematiche affrontate, di prossimità alle esigenze delle singole realtà aziendali e di accreditamento all'interno del Gruppo.

Q: Il GDPR assegna al DPO una posizione del tutto peculiare; tale figura, infatti, deve godere di autonomia e indipendenza avendo, allo stesso tempo, un canale privilegiato di comunicazione con il vertice aziendale. In una struttura di Gruppo, quale Mediobanca, com'è garantita l'autonomia e l'indipendenza del DPO?
Dott. P. Ginex: Il DPO è nominato dal Consiglio di Amministrazione della singola società per la quale opera e a tale organo riferisce periodicamente e ogni qual volta lo ritenga necessario. Le relazioni indirizzate al C.d.A. contengono informazioni sull'andamento delle attività, sulle principali criticità riscontrate e sulle progettualità in corso. Nel quotidiano, l'unità fornisce pareri e consulenza, partecipando ai progetti più rilevanti per la protezione di dati personali, ed effettua attività di controllo sul rispetto della regolamentazione

esterna ed interna. Le attività svolte sono oggetto di formalizzazione in note destinate al *senior management* e agli organi sociali. Da ultimo, deve essere ricordato come l'unità disponga di un proprio budget annuale, tipicamente utilizzato per la richiesta di pareri legali esterni e per il supporto in attività formative rivolte alla popolazione aziendale.

Q: Ascoltando con interesse le sue parole, possiamo dire che ci sia una grande attenzione al principio di accountability. Immaginiamo che l'attività di adeguamento al GDPR abbia tenuto ampiamente conto di questo principio, ma nel day-by-day come viene approcciata l'accountability?
Dott. P. Ginex: Il progetto di adeguamento al GDPR ha sicuramente tenuto ampiamente conto del principio di *accountability,* inteso come la responsabilizzazione del titolare del trattamento nell'adozione di comportamenti proattivi, atti a dimostrare la concreta istituzione di misure finalizzate ad assicurare l'applicazione del regolamento.
In tale contesto, grande attenzione è stata dedicata, *in primis*, alla tenuta aggiornata e puntuale del registro dei trattamenti, quale strumento di p*rivacy by design* e di individuazione di quei trattamenti che richiedono un *Data Protection Impact Assessment*. Si è poi provveduto alla revisione delle informative, delle nomine degli autorizzati e dei responsabili del trattamento, degli standard contrattuali e delle procedure, impostando al termine le attività di controllo volte a verificare l'effettiva applicazione delle misure tecniche e organizzative. Infine, sono stati adottati i necessari presidi per la formazione nel continuo dei dipendenti.
Ritengo però che il principio di *accountability*, che rappresenta la stella polare del nuovo *framework* normativo, abbia trovato un terreno decisamente fertile all'interno del nostro Gruppo, da sempre molto incline alla formalizzazione delle scelte. Tra le varie interpretazioni del termine *accountability* sorte *post* GDPR, ho trovato molto accattivante quella che, separando il termine in "account-ability", lo traduce con "capacità di rendere conto". Cerchiamo quindi di porci sempre nella condizione di poter rendicontare le soluzioni adottate e, soprattutto, i razionali che ci hanno condotto in una determinata direzione.
Questo approccio determina uno sforzo operativo importante che, in una prima fase, ritenevamo fosse necessario in preparazione di eventuali accessi ispettivi.
Col tempo, viceversa, abbiamo iniziato ad apprezzarne il valore anche in ottica di efficientamento interno, potendo contare su informazioni strutturate quando si presentano tematiche già affrontate nel passato.

Q: Un aspetto fondamentale che i titolari e i responsabili sono tenuti a considerare è quello della sicurezza dei dati personali, tenuto conto, ad esempio, del contesto, delle finalità e della natura dei trattamenti effettuati. In ragione di ciò, come si è organizzato il Gruppo a livello procedurale e organizzativo per rispettare le tempistiche sfidanti imposte dalla normativa per la gestione dei data breach?

Dott. P. Ginex: Tenuto conto che gli attacchi informatici e, più in generale, gli eventi che possono generare un *data breach* sono sempre più comuni a livello di sistema, le aziende devono essere in grado di dotarsi di misure di sicurezza e processi interni per affrontare tali minacce in maniera veloce e puntuale, riducendo al minimo gli eventuali impatti.

Un processo strutturato e ben rodato è quindi determinante per identificare nel più breve tempo possibile la migliore strategia di risoluzione.

Il processo che abbiamo disegnato vede il tempestivo coinvolgimento dell'unità Group Data Protection e la stretta collaborazione con la Funzione IT Risk & Cyber Security, deputata alla gestione della più ampia categoria degli incidenti di sicurezza ed *entry point* dell'intero processo. Alla nostra unità spetta il compito di qualificare gli incidenti come *data breach*, avvalendoci delle indicazioni e delle metodologie delle autorità europee, Comitato europeo per la protezione dei dati ed ENISA *in primis*, di valutare la necessità di notificare la violazione al Garante Privacy e di effettuare la comunicazione agli interessati.

Ciò che però non troviamo scritto nelle procedure è il fatto che, in caso di *data breach*, il DPO diviene il "collante" di un *iter* decisamente articolato, da portare a compimento in una tempistica predefinita e con la compartecipazione di una pluralità di attori. Difatti, le indispensabili analisi di sicurezza, il coinvolgimento degli *stakeholders* interni ed esterni, inclusa l'Autorità, i diversi adempimenti e i flussi informativi generano complessità e tensioni che il DPO deve essere in grado di gestire con grande capacità di ordine.

Q: Approfittando della sua disponibilità, vorremmo domandarle, in relazione alla sua esperienza nel ruolo, quali sono le difficoltà operative maggiormente riscontrate fino a questo momento.

Dott. P. Ginex: Quando si approccia la tematica delle difficoltà incontrate dal DPO, credo vada fatta una necessaria premessa, per ricordare come il GDPR sia una normativa ancora molto recente e come il Responsabile della protezione dei dati rappresenti una figura innovativa all'interno di ecosistemi organizzativi complessi, come lo sono le nostre aziende.

Un primo aspetto meritevole di attenzione è certamente correlato all'esigenza di attuare concretamente gli approcci metodologici definiti nella normativa

interna. Con riferimento alla *data retention*, ad esempio, abbiamo riscontrato da parte delle strutture impattate alcune ritrosie, o anche semplici timori, a cancellare i dati personali una volta raggiunti i tempi massimi di conservazione individuati.
Anche sul fronte del *data breach*, tematica della quale abbiamo parlato poc'anzi, penso che vi sia ancora della strada da fare nella capacità e sensibilità di individuazione dell'evento da parte dei singoli per l'avvio del processo di segnalazione. Noto infatti che le persone, probabilmente abituate al rilievo mediatico attribuito agli episodi di *data breach* informatico di rilevanti dimensioni, tendono a sottostimare, o addirittura a non considerare, situazioni che coinvolgono numeriche più ridotte, magari correlate a dati personali presenti su supporti cartacei.
Infine, con riferimento al principio di *privacy by design*, mi rendo conto che, talvolta, i meccanismi che prevedono il coinvolgimento del DPO fin dalla progettazione di una nuova iniziativa non garantiscono il pieno raggiungimento del risultato, costringendo le strutture a una revisione delle tempistiche di avvio del progetto per consentire i necessari approfondimenti sul fronte *data protection*.
Personalmente, ritengo che queste aree di miglioramento siano caratterizzate da una matrice comune, ovvero l'esigenza di migliorare progressivamente la cultura della protezione del dato personale. E questo, evidentemente, è un compito di cui il DPO deve farsi carico.

Q: L'ultima domanda prima di concludere. Al di fuori del suo ruolo di DPO, come applica le sue conoscenze in materia di protezione dei dati personali nella vita privata?
Dott. P. Ginex: Penso che l'incremento esponenziale dei trattamenti di dati personali tramite canali digitali e su piattaforme *online* offra grandi vantaggi e opportunità ma, allo stesso tempo, vada gestito, sia dai titolari del trattamento che dagli interessati, con grande responsabilità e coscienza. Le fondamenta sulle quali costruire relazioni corrette e durature mi sembrano rappresentate, senza allontanarmi troppo dai principi del GDPR, da un'informativa trasparente e comprensibile e dalla piena consapevolezza dell'interessato.
Sono quindi piuttosto contrario alla demonizzazione generalizzata nei confronti di determinate categorie di trattamenti, quali ad esempio quelli con finalità di *marketing*. Semplicemente, apprezzo un'informativa adeguata, scelgo da chi essere contattato e, ove io non sia più interessato, mi accerto di poter agevolmente revocare il mio consenso.