Maggio 2017

Gli istituti bancari al test del Regolamento privacy europeo

Giangiacomo Olivi, Partner, responsabile dipartimento IP&T, Laura Borelli, Trainee, dipartimento IP&T, DLA Piper

La protezione dei dati personali è e deve rimanere un tema di cruciale importanza per gli istituti bancari. La capacità di assicurare la riservatezza e la sicurezza dei dati bancari, inclusi i dati personali, rappresenta un fattore critico di successo, oltre a consentire di evitare l'applicazione di sanzioni destinate a divenire ancora più pesanti con l'applicazione della nuova normativa europea in materia di *privacy*.

Già da tempo il Garante per la protezione dei dati personali italiano è intervenuto a dettare delle regole *ad hoc* per il trattamento dei dati personali nell'ambito delle operazioni bancarie. Si fa riferimento al provvedimento n. 192/2011 recante "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie*", seguito dall'emanazione del provvedimento n. 357/2013, con cui il Garante ha definito il quadro operativo della delibera n. 192/2011, chiarendone l'ambito di applicazione.

Tuttavia, il quadro attuale è destinato a cambiare sensibilmente nel corso del prossimo anno. In data 24 maggio 2016, al termine di un intenso iter legislativo durato quattro anni, è entrato in vigore il testo definitivo del Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali (il cosiddetto "GDPR"), che diventerà definitivamente applicabile in via diretta in tutti i Paesi dell'Unione Europea a partire dal 25 maggio 2018.

Il GDPR abroga la precedente Direttiva Europea 95/46/CE, attuata in Italia con il Decreto Legislativo n. 196 del 30 giugno 2003 recante il "Codice Privacy" in materia di protezione dei dati personali, introducendo una vera e propria rivoluzione degli adempimenti *privacy* per tutte le imprese e gli istituti bancari che offrono i propri servizi in Europa. Obiettivo della nostra indagine sarà quello di individuare i principali cambiamenti che l'adeguamento alla nuova normativa privacy comporterà per le banche italiane.

Al fine di dar concretezza alle novità introdotte dal GDPR e chiarire alcune delle ambiguità in esso contenute, già da alcuni mesi il Gruppo dei Garanti Europei (Article

29 Data Protection Working Party, ovvero "WP29")[1] si è attivato per realizzare delle linee guida all'applicazione pratica del nuovo dettato normativo[2].

In questo contesto, anche il Garante italiano ha ritenuto opportuno offrire delle indicazioni al fine di facilitare l'applicazione del nuovo quadro regolatorio a livello locale. A tal fine, il Garante ha pubblicato lo scorso 28 aprile la prima "*Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali*", un prontuario destinato a supportare i soggetti pubblici e le imprese che stanno affrontando il passaggio alla nuova normativa privacy. In vista dell'applicazione del GDPR, il Garante ha inoltre avviato una serie di incontri con alcuni soggetti pubblici e privati con l'obiettivo tra le altre cose di fornire indicazioni sulle prassi da seguire.

Nell'ambito della Guida, il Garante individua sei questioni principali, specificando per ciascuna di esse gli elementi di novità e di continuità rispetto agli elementi del Codice Privacy e offrendo anche consigli pratici sui possibili approcci da adottare in vista della piena applicazione del GDPR. Risulta utile ai fini della nostra indagine ripercorrere tali questioni con una logica analoga a quella della Guida al GDPR, in modo da evidenziare cosa cambierà rispetto all'attuale disciplina.

Fondamenti di liceità del trattamento

Per essere lecito, il trattamento di dati personali deve essere fondato su un'idonea base giuridica. Come già previsto dal Codice Privacy, il consenso dell'interessato può consistere una valida base per il corretto trattamento dei dati. Il consenso deve essere libero, specifico, informato e manifestato mediante "*dichiarazione o azione positiva inequivocabile*"[3]. In questo senso, non possono essere intesi come volti a prestare il consenso il silenzio, l'inattività o la preselezione di caselle.

Rispetto alla normativa precedente, il GDPR non richiede né la forma scritta né la documentazione per iscritto del consenso al trattamento, bensì che il titolare del trattamento sia "*in grado di dimostrare*" che l'interessato ha acconsentito a tale trattamento. In questo senso, risulta in ogni caso consigliabile, a fini probatori e soprattutto ai fini di conformità con il principio di *accountability* o

[1] Il Gruppo è stato istituito dall'art. 29 della Direttiva 95/46/CE ed è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

[2] Il 13 dicembre scorso il WP29 ha approvato le prime tre linee guida relative rispettivamente al responsabile per la protezione dei dati (Data Protection Officer "DPO"), al diritto alla portabilità dei dati e all'autorità capofila, in vista della applicazione da parte degli Stati membri del GDPR. A desse si sono aggiunte lo scorso 4 aprile le linee guida in materia di valutazione d'impatto sulla privacy volte a fornire un ausilio ai titolari del trattamento nell'individuazione delle operazioni di trattamento che richiedono l'effettuazione di una valutazione d'impatto

[3] Considerando 32, Art. 4 n. 11

responsabilizzazione, tenere traccia del consenso conferito in relazione a uno specifico trattamento.

Il legittimo interesse può rappresentare una base alternativa al consenso per il trattamento dei dati. Mentre il Codice Privacy ammette la possibilità di trattare i dati di un soggetto interessato in assenza del suo consenso "*nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato*"[4], con il GDPR viene meno la necessità di un provvedimento del Garante. Spetta, quindi, al titolare del trattamento la valutazione circa la prevalenza del legittimo interesse del titolare o del terzo rispetto ai diritti e alle libertà dell'interessato. Tuttavia, non è detto che il legittimo interesse costituisca una base solida per il trattamento dei dati, non essendo sottoposto a validazione di legge o del garante, come nel regime precedente. In questo senso, la presunzione di legittimità potrebbe essere impugnata dagli interessati e, in tal caso, il trattamento dovrebbe essere sospeso salvo che il titolare non sia in grado di dimostrare l'esistenza di valide ragioni che ne richiedono la continuazione e che prevalgono sui diritti di tali interessati.

Informativa

I contenuti dell'informativa sono elencati in modo tassativo dal GDPR e in parte sono più ampi rispetto al Codice Privacy. Tra le altre, una novità rilevante riguarda l'esigenza di riportare in informativa l'indicazione del periodo per il quale i dati raccolti e trattati verranno conservati.

Con il GDPR cambia la forma dell'informativa, che deve essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Essa deve essere fornita, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto se fornita al pubblico tramite un sito web[5]. Inoltre, il GDPR prevede che i contenuti dell'informativa possano essere presentati in modo sintetico tramite l'impiego di icone standardizzate che consentano di offrire un quadro d'insieme facilmente visibile, intelligibile e chiaramente leggibile del trattamento da effettuare, sempreché tali icone siano impiegate in combinazione con un'informativa estesa

Diritti degli interessati

Il GDPR amplia gli esistenti diritti degli interessati con una gamma di diritti nuovi o "rinnovati". Tra gli altri, una delle novità più significative riguarda il diritto di ottenere la cancellazione dei dati personali senza ingiustificato ritardo in presenza di specifici presupposti ("*right to be forgotten*" o diritto all'oblio). L'attribuzione di tale diritto comporta notevoli implicazioni per il titolare del trattamento che dovrà adottare

[4] Art. 24 comma 1 lett. g) Codice Privacy
[5] Considerando 58

soluzioni tecniche in grado di assicurare la cancellazione automatica dei dati non solo sul singolo sistema aziendale tramite il quale i dati sono stati raccolti, ma anche su tutti gli altri sistemi all'interno dei quali tali dati sono eventualmente circolati / trattati.

Altra innovazione con un importante impatto dal punto di vista pratico riguarda l'introduzione del diritto alla portabilità, vale a dire il diritto di ricevere i propri dati (compresi i dati relativi all'estratto conto) in un formato strutturato, di uso comune e leggibile da dispositivo automatico e ottenerne la trasmissione ad un altro fornitore di servizi. L'esigenza di dar corso alle richieste di portabilità degli interessati impone tanto un adeguamento delle politiche interne quanto una mappatura dei dati e dei flussi di dati trattati da parte del titolare del trattamento. Tale operazione di mappatura non solo consentirebbe di rispettare il dettato normativo e la volontà dell'interessato richiedente, ma anche di aver una maggior controllo in sede di trasmissione dei dati di modo da limitare o evitare la divulgazione di informazioni ulteriori, che potrebbero consistere anche in informazioni confidenziali o segreti industriali, ad altri titolari eventualmente concorrenti.

Titolare, responsabile e incaricato

Quanto alle figure coinvolte nel trattamento, il GDPR definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui al Codice Privacy. Nuove regole si applicheranno sia ai casi in cui la banca rivesta il ruolo di co-titolare del trattamento insieme alla società di gestione dei sistemi informativi tramite i quali vengono elaborati i dati dei clienti sia a quelli in cui la banca rivesta il ruolo di unica titolare del trattamento (per i casi pratici si faccia riferimento alle Prescrizioni del Garante). In particolare, con riferimento alla prima ipotesi, il GDPR ha introdotto delle nuove regole in materia di contitolarità del trattamento, secondo le quali i titolari devono definire specificamente con un atto giuridicamente valido il rispettivo ambito di responsabilità e i rispettivi compiti con riferimento all'esercizio dei diritti degli interessati, salva la responsabilità solidale dei contitolari nei confronti degli interessati indipendentemente da tale ripartizione di compiti e obblighi. Con rifermento alla seconda ipotesi, occorre invece tener conto che il GDPR impone al titolare di nominare formalmente il responsabile del trattamento tramite un apposito contratto di trattamento dei dati, nel quali siano indicati la natura, la durata e la finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento, anche ai fini dell'adempimento degli obblighi in caso di *data breach* e della cancellazione dei dati al termine della fornitura dei servizi.

Va in ultimo rilevato che, benché la figura dell'incaricato del trattamento rappresenti una specificità tutta italiana e non sia espressamente prevista all'interno del GDPR, il Garante ne ammette la compatibilità con la nuovo normativa e, anzi, ritiene consigliabile mantenere tale figura. Continueranno, quindi, ad applicarsi le relative

disposizioni in materia di tracciamento delle operazioni effettuate dagli incaricati del trattamento contenute nelle Prescrizioni del Garante.

Accountability e DPO

Rispetto all'attuale disciplina di riferimento in materia di protezione dei dati personali (più incentrata sui diritti dell'interessato), il GDPR introduce un quadro normativo incentrato sugli obblighi e sulla responsabilizzazione del titolare e del responsabile del trattamento. In tale contesto, uno dei principi cardine su cui si basa il GDPR consiste per l'appunto nel principio di *accountability* o responsabilizzazione. Tale principio si traduce, da un lato, nell'adozione di misure tecniche e modelli organizzativi atti a garantire che la gestione e conservazione dei dati avvenga in maniera conforme ai principi di protezione dei dati personali e, dall'altro, nella capacità di dimostrare la conformità delle operazioni di trattamento effettuate a tali principi[6].

Più dettagliamene, il suddetto principio si estrinseca, anzitutto, nella necessità di integrare la protezione dei dati personali in tutti i processi e nella cultura dell'organizzazione tramite l'adozione di politiche interne e misure che soddisfino i principi della protezione dei dati fin dalla progettazione (*privacy by design*) e della protezione dei dati per impostazione predefinita (*privacy by default*).

In adempimento ai summenzionati principi, il titolare del trattamento sarà tenuto a svolgere un'analisi preventiva dell'impatto dell'operazione di trattamento (*Data Privacy Impact Assessment*, si seguito "DPIA") laddove il trattamento possa presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati. Tale adempimento è introdotto dal GDPR in sostituzione dell'obbligo di verifica preliminare previsto all'art. 17 del Codice Privacy. L'obiettivo del DPIA è quello di consentire al titolare di individuare e applicare sin dalla progettazione del servizio o prodotto i correttivi opportuni per la prevenzione del rischio e ridurre i costi e i danni reputazionali che potrebbero derivare dalla violazione della normativa in materia di protezione dei dati. Lo svolgimento del DPIA è prodromico all'eventuale consultazione preventiva con il Garante, da effettuarsi obbligatoriamente nei casi in cui, all'esito del DPIA, risulti impossibile individuare delle misure "*opportune in termini di tecnologia disponibile e costi di attuazione*"[7] atte ad attenuare sufficientemente il rischio del trattamento.

[6] Articolo 5, comma 2: Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

[7] Considerando 84 del GDPR: "*Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure*

Quanto alle misure di sicurezza, il GDPR richiede che le stesse siano in grado di garantire un livello di sicurezza "*adeguato al rischio*" del trattamento. Il GDPR offre una lista aperta di misure applicabili, lasciando al titolare e al responsabile del trattamento la valutazione circa le misure applicabili in concreto, tenuto conto dei rischi specificamente individuati in relazione all'operazione di trattamento. Nell'individuare le misure concretamente applicabili, gli istituti bancari dovranno in ogni caso tener conto tanto delle specificità previste dalle Disposizioni di vigilanza per le banche in materia di conformità alle norme della Banca d'Italia, quanto delle disposizioni contenute nelle Prescrizioni in materia di tracciamento degli accessi ai dati bancari dei clienti, tempi di conservazione dei relativi file di log e implementazione di *alert* di rilevazione di intrusioni o accessi anomali ai dati bancari.

Sempre in un'ottica di responsabilizzazione, il GDPR introduce la figura del responsabile per la protezione dei dati (*Data Protection Officer*, di seguito "DPO"). Il DPO è un soggetto con competenze giuridiche, informatiche, di *risk management*, di analisi dei processi che ha il compito di valutare, organizzare e governare la gestione del trattamento dei dati nel rispetto della nuova normativa. Tale figura è stata creata per supportare il titolare e il responsabile del trattamento nell'adempimento al GDPR ed è destinata ad assumere particolare importanza nell'ambito degli istituto bancari. Maggiori ragguagli circa le caratteristiche soggettive (competenze professionali, garanzie di indipendenza e inamovibilità) e i compiti del DPO sono contenute nelle linee guida sul DPO recentemente adottate dal WP29.

Il principio di responsabilizzazione si estrinseca, infine, nell'obbligo sia per i titolari che per i responsabili del trattamento di tenere un registro delle attività di trattamento, strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'organizzazione.

Trasferimento internazionale di dati

Il GDPR ha confermato l'approccio attualmente vigente in materia di flussi di dati al di fuori dell'Unione europea, prevedendo che tali flussi sono vietati, in linea di principio, salvo che intervengano specifiche garanzie, quali una decisione di adeguatezza del Paese terzo coinvolto riconosciuta tramite decisione della Commissione europea, l'esistenza di garanzie adeguate di natura contrattuale o pattizia (i.e. le norme vincolanti d'impresa o *binding corporate rules* e le clausole contrattuali modello) o eventuali deroghe a suddetto divieto.

Viene meno del requisito dell'"autorizzazione nazionale", nel senso che il trasferimento verso un Paese terzo "adeguato" in base alla decisione assunta dalla Commissione europea ovvero a delle clausole contrattuali modello o di norme vincolanti d'impresa potrà avere inizio senza attendere l'autorizzazione Garante. Tuttavia, tale autorizzazione

---

opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo".

sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali *ad-hoc* (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorità pubbliche.

Un altro cambiamento rilevante, soprattutto per i gruppi bancari, consiste nella possibilità di individuazione un'unica autorità capofila, vale a dire un'unica autorità di controllo di rifermento a livello comunitario, che deve fungere da "sportello unico" per i trattamenti transnazionali laddove il titolare o il responsabile tratti dati personali in più stabilimenti nell'UE o offra prodotti o servizi in più Paesi Ue anche a partire da un solo stabilimento. Si tratta di un elemento importante del nuovo quadro normativo e sarà determinante fare riferimento ai chiarimenti forniti dal WP29 nella apposite linee guida del 13 dicembre 2016, come aggiornate lo scorso 5 aprile per comprendere nel dettaglio le modalità di individuare dell'autorità capofila.

Le novità del GDPR sono molteplici. L'allineamento fra la normativa nazionale e le disposizioni del GDPR richiederà un grande sforzo alle banche italiane ed europee ed imporrà un salto di qualità significativo nell'approccio alla *privacy*, nel sistema delle responsabilità e nell'adozione di misure di sicurezza, con un impatto trasversale su tutti i processi aziendali. E' bene iniziare già da ora a definire gli *step* necessari per uniformarsi al GDPR e rivedere la *data governance*, in modo tale da cogliere appieno le opportunità derivanti dalle nuove tecnologie, senza rischiare sanzioni che con il GDPR potrebbero raggiungere anche 4% del fatturato globale annuo.

Copyright dirittobancario.it