Verbale di Accordo
applicativo delle prescrizioni del Garante
in materia di tracciabilità delle operazioni bancarie

Verona, il 28/05/2014

tra

il Banco Popolare in qualità di Capogruppo, anche in nome e per conto delle società del Gruppo

e

le Delegazioni di Gruppo Dircredito-FD, Fabi, Fiba-Cisl, Fisac-Cgil, Sinfub, Ugl-Credito e Uilca

unitamente

agli Organismi Sindacali Aziendali delle OO.SS. Dircredito-FD, Fabi, Fiba-Cisl, Fisac-Cgil, Sinfub, Ugl-Credito e Uilca, costituiti presso le società del Gruppo,

premesso che:

- il d.lgs. 30 giugno 2003, n. 196, rubricato "*Codice in materia di protezione dei dati personali*" stabilisce che chiunque ha diritto alla protezione dei dati personali che lo riguardano e disciplina, tra l'altro, compiti e funzioni del Garante per la protezione dei dati personali;

- il Garante per la protezione dei dati personali, ha il compito di prescrivere, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento dei dati conforme alle disposizioni vigenti;

- il Garante per la protezione dei dati personali ha emanato, in data 12 maggio 2011, il Provvedimento n. 192 avente ad oggetto "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie*";

- in data 18 luglio 2013, lo stesso Garante ha emanato il Provvedimento n. 357 e ne ha differito il termine previsto per l'entrata in vigore;

- il Provvedimento – che entra in vigore, a seguito del predetto differimento, in data 3 giugno 2014 – è finalizzato a garantire il rispetto dei principi in materia di protezione dei dati personali ai sensi del Codice sopra citato, in ordine ai temi della «circolazione» delle informazioni riferite ai clienti in ambito bancario e della «tracciabilità» delle operazioni bancarie" e detta, ai sensi dell'art. 154, comma 1, lett. c), prescrizioni in relazione al trattamento dei dati personali della clientela effettuato dai dipendenti delle "banche, incluse quelle facenti parte di gruppi, delle società, anche diverse dalle banche, purché siano parte di tali gruppi, stabiliti sul territorio nazionale";

- detto Provvedimento riguarda le operazioni relative ai clienti degli istituti bancari di cui all'alinea che precede, sia quelle che comportano movimenti di denaro sia quelle di sola consultazione (cd. "inquiry");

- il Provvedimento si applica a tutti i lavoratori "incaricati dall'azienda dei trattamenti" riconducibili nell'applicazione del Provvedimento e specificamente, come chiarito successivamente dal medesimo Garante nel Provvedimento in data 18 luglio 2013 n. 357, "quali che siano la qualifica, le competenze, gli ambiti di operatività e le finalità dei trattamenti che sono tenuti a svolgere";

- sempre secondo detto Provvedimento, è prescritta l'adozione di "idonee soluzioni informatiche" che comprendono "la registrazione dettagliata in un apposito *log* delle informazioni riferite alle operazioni bancarie" e sempre che non si tratti di dati "in forma aggregata non riconducibili a singolo cliente";

- il Provvedimento medesimo prescrive altresì che le misure previste siano adottate "nel rispetto della vigente disciplina in materia di controllo a distanza dei lavoratori ex art. 4, comma 2, della legge 20 maggio 1970, n. 300";

- è richiesto altresì dal Garante che siano attivati "specifici alert" relativi alle operazioni di *inquiry* eseguite dagli incaricati volti "a rilevare intrusioni o accessi anomali ai dati bancari, tali da configurare eventuali trattamenti illeciti";

- le misure del Provvedimento "debbono essere osservate pure dalle società che operano in *outsourcing* - anche quando non appartengono al Gruppo bancario - allorché l'attività esternalizzata sia connessa all'esecuzione di rapporti contrattuali (intercorrenti tra banca e cliente) e richieda l'utilizzo di funzioni applicative a supporto dell'operatività bancaria";

- in data 15 aprile 2014 è stato sottoscritto l'accordo quadro nazionale sull'applicazione del Provvedimento del Garante per la protezione dei dati personali del 12 maggio 2011, n. 192, che qui si dà per integralmente richiamato, e che definisce lo schema generale di accordo da utilizzare per la sottoscrizione di intese ex art. 4, comma 2, Legge n. 300 del 1970 in specifica attuazione del Provvedimento in oggetto e prevede che il confronto a livello di gruppo sia finalizzato alla verifica della coerenza di quanto illustrato da parte aziendale con le vigenti disposizioni in materia e con l'accordo quadro nazionale medesimo;

- le Parti hanno effettuato il confronto, a livello di Gruppo nonché con gli Organi di Coordinamento Aziendale, previsto dall'accordo quadro nazionale, in particolare concernente le caratteristiche del sistema di tracciabilità progettato da parte aziendale, sulla base delle prescrizioni del Garante e di quanto emerso in sede di confronto delle Parti nazionali,

tutto ciò premesso, le Parti convengono quanto segue:

1. Le premesse sono parte integrante e sostanziale del presente Accordo.

2. Il presente Accordo in materia di tracciabilità delle operazioni bancarie si applica dal 3 giugno 2014, secondo le prescrizioni del Garante, nelle unità organizzative delle aziende facenti parte del Gruppo societario Banco Popolare. Al medesimo è allegata la scheda tecnica presentata dal Banco Popolare in qualità di Capogruppo, che altresì formalizza le dichiarazioni di cui al punto 3 che segue.

3. <u>*Dichiarazioni e impegni di parte aziendale*</u>

- Le soluzioni tecnologiche individuate, che saranno attivate a partire dal 3 giugno 2014, sono rispondenti alle prescrizioni del Garante e coerenti con le linee guida di ABI-LAB condivise tra i principali Gruppi bancari. Tali soluzioni assicureranno l'adeguato controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi *data-base* utilizzati.
- I sistemi informativi saranno impostati ai fini della registrazione dettagliata, in un apposito *log*, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari da tutti gli "incaricati del trattamento".
- In particolare, i file di *log* tracceranno, per ogni operazione di accesso ai dati bancari effettuata da un "incaricato", esclusivamente le seguenti informazioni in stretta aderenza ai requisiti indicati dal Garante in termini di dati bancari raccolti:
  - il codice identificativo del soggetto "incaricato" che ha posto in essere l'operazione di accesso;
  - la data e l'ora di esecuzione;
  - il codice della postazione di lavoro utilizzata;
  - il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato;
  - la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata.
- I *log* di tracciamento delle operazioni di *inquiry* saranno conservati per un periodo di 24 mesi dalla data di registrazione dell'operazione, fatte salve esigenze di forza maggiore. Oltre tale limite temporale la conservazione è ammessa in presenza di specifici vincoli di legge in materia.
- Come espressamente richiesto dal Garante, saranno attivati "specifici alert" finalizzati ad individuare "comportamenti anomali o a rischio" relativi alle operazioni di *inquiry* eseguite dagli "incaricati del trattamento".
- Sempre in conformità alle prescrizioni del Garante:
  - la gestione dei dati bancari sarà oggetto, con cadenza almeno annuale, di un'attività da parte dei titolari del trattamento volta alla verifica costante della rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme tempo per tempo vigenti;
  - l'attività di controllo prescritta dal Provvedimento sarà demandata a personale diverso da quello cui è affidato il trattamento dei dati bancari dei clienti;

- specificamente, i controlli delle competenti strutture di *audit* riguarderanno anche le verifiche a posteriori, a campione o a seguito di allarme derivante da sistemi di *alerting* e di *anomaly detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati e sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento, e altresì le verifiche periodiche sulla corretta conservazione dei *file di log* per il periodo sopra previsto;
- l'attività di controllo verrà adeguatamente documentata in modo tale che sarà sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

4. In merito alla previsione del Garante concernente l'apposita informativa (art. 13 d.lgs. n. 196 del 2003) sulle procedure adottate e sui connessi adempimenti, il Banco, in qualità di Capogruppo, tenuto ad ottemperare a tale previsione, porterà a conoscenza di tutti i lavoratori del Gruppo l'informativa medesima mediante pubblicazione nel portale aziendale, unitamente a comunicazione personale di avviso. Conformemente a quanto previsto nell'accordo quadro nazionale, andranno previste, nell'ambito di quanto stabilito dall'art. 72 del CCNL 19 gennaio 2012, specifiche attività formative retribuite per i lavoratori relativamente alla materia, rientrante nella più vasta tematica della 'privacy'.

5. In sede di Gruppo, con la partecipazione dei Coordinamenti Aziendali, verranno effettuati, d'intesa tra le Parti, incontri di verifica annuali in merito all'applicazione dell'Accordo in materia (la prima verifica sarà prevista entro il 31.03.2015).
   Nella medesima sede di verifica di cui sopra, alle Organizzazioni Sindacali firmatarie della presente intesa saranno fornite informazioni in ordine alla/e Unità Organizzativa/e cui è affidato il trattamento dei dati bancari dei clienti in base a quanto previsto dal provvedimento di che trattasi nonché sulle modalità di indagine a campione.

Per quanto altro non espressamente richiamato nel presente Accordo, si fa rinvio alle prescrizioni del Garante.

Ai sensi delle vigenti discipline legislative, ed in particolare della facoltà riconosciuta nell'ambito della contrattazione di secondo livello per la regolazione delle materie inerenti all'organizzazione del lavoro e della produzione, con riferimento, tra l'altro, alla "introduzione di nuove tecnologie", il presente Accordo - nello spirito in tal senso espresso dalle parti nazionali firmatarie dell'accordo quadro del 15 aprile 2014 - viene stipulato con le Delegazioni di Gruppo di cui all'art. 25 dell'Accordo di settore in materia di libertà sindacali 7.7.2010 e con gli Organi di Coordinamento di cui all'art. 24 del CCNL 19.01.2012.

Banco Popolare

Le Delegazioni di Gruppo e gli Organi di Coordinamento Aziendali

Dircredito-FD .....

Fabi .....

Fiba-Cisl .....

Fisac-Cgil .....

Sinfub .....

Ugl-Credito .....

Uilca .....

Allegato all'Accordo applicativo delle prescrizioni del Garante in materia di tracciabilità delle operazioni bancarie nelle aziende facenti parte del Gruppo societario Banco Popolare

SCHEDA TECNICA

Specifiche tecniche del sistema di tracciamento nel Gruppo BP

Le logiche assunte, riferentesi alle Linee Guida ABI-LAB sull'argomento razionalizzate al contesto operativo, sono state le seguenti:

- stretta aderenza ai requisiti Garante in termini di dati bancari raccolti;
- focalizzazione sulla individuazione delle sole operazioni di consultazione effettuate dagli incaricati (*inquiry*), con tempi di conservazione al minimo richiesto (24 mesi);
- impiego di una struttura SIEM (*Security Information and Event Management*) in grado di fornire quantitativi di sicurezza in termini di riservatezza ed inalterabilità dei dati raccolti e conservati;
- individuazione di un insieme minimale di indicatori (*alert*) in linea con il sistema bancario, finalizzati alla produzione di semplici segnalazioni aggregate di eventuali comportamenti potenzialmente anomali o a rischio, relativi alle operazioni di *inquiry* eseguite dagli incaricati.

Le misure di natura tecnologica implementate per i trattamenti condotti sugli elementi di informazione presenti si declinano nelle seguenti attuazioni progettuali:

- strutturazione architetturale della soluzione in ambiti di lavoro disaccoppiati in relazione a: 1) raccolta (*logging area*), 2) elaborazione (*staging area*), 3) conservazione e fruizione delle informazioni (SIEM area);
- applicazione di soluzioni tecniche in grado di catturare le informazioni prescritte tramite automatismi sistemistici-applicativi;
- impiego del sistema SIEM per conservare le registrazioni delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari e per correlare le informazioni raccolte secondo le logiche di monitoraggio impostate (*alert*).

Le informazioni oggetto del Provvedimento, nel loro iter di raccolta ed elaborazione vengono protette in modo opportuno con tecniche di compressione e limiti d'accesso.

Le elaborazioni accentrate ed il raccordo tra le diverse Società del Gruppo avvengono in modo *batch* tramite flussi di archivi. I dati nel SIEM vengono poi protetti da una doppia cifratura.

Caratteristiche degli *alert*

Riguardo la previsione dei meccanismi di *alerting* sulle informazioni raccolte e conservate, finalizzati alla mitigazione del rischio di trattamenti illeciti da parte degli operatori incaricati, come richiesto dal Garante, sono state individuate:

- fascia oraria in cui è stata eseguita l'operazione (giorni lavorativi o non lavorativi, orario d'ufficio o extra);
- competenza territoriale dell'operatore che effettua la richiesta;
- ruolo degli operatori;
- concentrazione di inquiry in un determinato intervallo temporale.

L'*alert* è generato automaticamente quando tali parametri e/o una combinazione di essi superano una soglia prestabilita rispetto frequenze e livelli di riferimento definiti ad una normale operatività.

Nel rispetto del principio della segregazione dei compiti previsti dalla normativa, i profili autorizzativi ed i diritti di accesso ai dati bancari sono adeguatamente gestiti e controllati, di conseguenza non possono verificarsi transazioni al di fuori dei ruoli organizzativi autorizzati.