ACCORDO SULL'APPLICAZIONE DEL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 12 MAGGIO 2011, N. 192

Il 23 MAGGIO 2014

tra

Banca Monte dei Paschi di Siena Spa

e

gli organi di coordinamento di

Dircredito – Fabi – Fiba/Cisl – Fisac/Cgil – Sinfub – Ugl Credito - Uilca

Premesso che

1. 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;

2. 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;

3. 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;

4. il Provvedimento – che entrerà in vigore il 3 giugno 2014 – è finalizzato a "garantire il rispetto dei principi in materia di protezione dei dati personali ai sensi del Codice, 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 di tali 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;

5. il Provvedimento riguarda le operazioni relative ai clienti degli istituti bancari di cui al punto che precede, "sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, c.d. inquiry";

6. il Provvedimento si applica a tutti i lavoratori "incaricati dall'azienda dei trattamenti" riconducibili nell'ambito di applicazione del Provvedimento n. 192, come chiarito nel successivo Provvedimento n. 357, "quali che siano la qualifica, le competenze, gli ambiti di operatività e le finalità dei trattamenti che sono tenuti a svolgere";

7. il Provvedimento, "al fine di assicurare il controllo delle attività svolte sui dati dei clienti e dei potenziali clienti da ciascun incaricato del trattamento", prescrive l'adozione di "idonee soluzioni informatiche" per il controllo dei "trattamenti condotti sui singoli elementi di informazione presenti nei diversi database"; "tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente";

8. il Provvedimento, in particolare, stabilisce che "i file di log devono tracciare, per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:

- ✓ 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 del rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata (es. numero del conto corrente, fido/mutuo, deposito titoli)";

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

10. l'art. 4, comma 2, l. 20 maggio 1970, n. 300 prevede che gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati previo accordo sindacale con le rappresentanze sindacali aziendali;

11. l'art. 114 d.lgs. 30 giugno 2003, n. 196 stabilisce che "Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300";

12. il Provvedimento richiede 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";

13. il Provvedimento definisce "un quadro unitario di misure necessarie e opportune" per tutte le banche e i gruppi bancari di cui al punto 4 che precede;

14. 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";

15. considerate le peculiari caratteristiche del provvedimento, con l'accordo quadro nazionale del 15.04.2014 sull'applicazione del provvedimento del garante per la protezione dei dati personali del 12 maggio 2011, n. 192, ABI e le OSL di settore hanno definito lo "schema generale di accordo" da utilizzare nelle aziende del credito per la stipulazione di intese ex art.4, comma 2, l. n. 300 del 1970 in specifica attuazione del provvedimento in oggetto;

16. tale accordo stabilisce inoltre che il confronto aziendale o di gruppo è finalizzato alla verifica della coerenza delle proposte aziendali con le vigenti disposizioni in materia e con l'accordo quadro stesso.

tutto ciò premesso,

le Parti intendono favorire l'attuazione del surrichiamato Provvedimento del Garante, fermo il relativo ambito di applicazione, in relazione alle previsioni dell'art. 4, comma 2, l. n. 300 del 1970, nel rispetto delle esigenze di tutela individuale, di quelle aziendali, nonché delle specifiche prerogative sindacali;

e conseguentemente convengono quanto segue:

- La premessa forma parte integrante e sostanziale del presente Accordo aziendale.

- La banca adotta idonee soluzioni informatiche per il controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database, ai sensi di quanto prescritto dal Garante per la protezione dei dati personali con il Provvedimento n. 192 del 12 maggio 2011.

- I sistemi informativi sono 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 devono tracciare per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni: 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 (es. numero del conto corrente, fido/mutuo, deposito titoli) del cliente a cui si riferisce l'operazione effettuata. Banca MPS, integra le informazioni sopra riportate con il codice e la tipologia di operazione attivata.

- Banca Mps in ottemperanza del punto 3 del Provv. 357/2013 del Garante per la Protezione dei Dati Personali, inerente gli accessi massivi, registra inoltre il "dettaglio della richiesta", ovvero i parametri di selezione che sono stati utilizzati per eseguire l'accesso ai dati.

- I log di tracciamento delle operazione di inquiry sono 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.

- La gestione dell'operatività avverrà attraverso un'apposita piattaforma informatica che raccoglie i dati tracciati dai sistemi informativi e una volta normalizzati (resi omogenei), li trasferisce in un log privacy, dove vengono conservati come specificato al punto precedente. Attraverso questa piattaforma informatica vengono inoltre costruiti gli alert sulla base di regole e campionature predefinite, i dati rilevati vengono elaborati e sono fornite le opportune evidenze per i controlli.

- Le specifiche tecniche di cui sopra, riportate nell'allegato, formano parte integrante del presente accordo. Le eventuali future rilevanti modifiche costituiranno anch'esse parte integrante del presente accordo e saranno oggetto di illustrazione in apposito incontro sindacale.

- Come espressamente richiesto dal Garante, sono attivati "specifici alert" finalizzati ad individuare potenziali "comportamenti anomali o a rischio" relativi alle operazioni di inquiry eseguite dagli incaricati del trattamento. BMPS ha identificato sulla base dei parametri e delle informazioni disponibili i seguenti quattro alert:

    1. Accesso eseguito da un singolo operatore ai dati bancari di un cliente non di competenza;
    2. Accesso di un singolo operatore a dati bancari di un cliente (NDC) in modo ripetuto.
    3. Accesso di un singolo operatore ai rapporti di un cliente (NDC) di competenza e ai suoi NDC collegati in modo ripetuto.
    4. Accesso di un singolo operatore ai dati bancari dei clienti in modo massivo.

La competenza corrisponde al contesto organizzativo in cui un dipendente è chiamato ad agire in forza dell'incarico conferitogli e prevede l'esecuzione da parte dell'operatore di adempimenti coerenti, per tipologia, con lo stesso incarico.

I comportamenti che generano segnalazioni sono quelli che si discostano dalla corretta operatività che deve essere posta in essere per la normale gestione delle attività assegnate e/o per il seguimento della relazione con i clienti, ivi comprese le attività diverse da quelle di front end, in particolare quelle di supporto e B.O..

Il sistema di alert non considera, in via generale, gli accessi ai dati non aventi valenza patrimoniale ed economica.

Ai sensi del Provvedimento:

- "la gestione dei dati bancari è oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti";
- "l'attività di controllo è demandata ad una unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti";
- "i controlli comprendono anche verifiche a posteriori, a seguito di allarme derivante da sistemi alerting e di anomaly detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte altresì verifiche periodiche sulla corretta conservazione dei file di log per il periodo" sopra previsto;
- "l'attività di controllo è adeguatamente documentata in modo tale che sia 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".

L'impostazione del sistema di alerting e controlli prevede:

- una rilevazione automatica degli eventi da verificare;
- controlli di linea – per valutare gli eventi (Titolare/Responsabile strutture);
- controlli di linea di livello superiore (DOR per la rete; Servizio Compliance per la Direzione Generale);

- controlli di secondo livello – Funzione Compliance;

In particolare, nell'ambito del sistema in argomento, il processo di controllo prende avvio sulla base dei risultati ottenuti mediante la rilevazione automatica di cui sopra.

La prima valutazione è effettuata dal Responsabile della struttura a cui appartiene l'incaricato che ha operato l'accesso. Nel caso in cui sussistano elementi che necessitano di ulteriori valutazioni verranno coinvolte le strutture gerarchicamente o funzionalmente sovraordinate a quella a cui appartiene l'operatore.

La Funzione di Controllo di secondo livello (Compliance) monitorerà i comportamenti e i controlli posti in essere dalle strutture centrali e periferiche.

Qualora le funzioni che avviano il processo di controllo debbano assumere informazioni dai soggetti interessati, necessarie per la definizione della segnalazione, la richiesta di chiarimenti sarà tempestivamente comunicata agli interessati stessi.

Nel caso in cui ne vengano ravvisati i presupposti la pratica è inoltrata alla Funzione Compliance che valuta l'eventuale applicazione delle misure opportune.

Nel caso in cui l'azienda ritenesse necessario introdurre significative variazioni agli strumenti di cui al presente accordo verrà effettuato un incontro preventivo nel quale le Parti valuteranno congiuntamente la conseguente eventuale necessità di integrare il presente accordo.

I lavoratori incaricati sono informati delle procedure adottate e dei connessi adempimenti tramite apposita informativa (art. 13 d.lgs. n. 196 del 2003), che sarà portata a conoscenza di tutti i lavoratori tramite e-mail. Inoltre, nell'ambito di quanto previsto dall'art. 72 del CCNL 19 gennaio 2012, sarà predisposto un corso di formazione on line a fruizione obbligatoria retribuita per tutti i dipendenti, al fine di far conoscere il Provvedimento del Garante e le sue applicazioni, che prevede un test finale di verifica dell'apprendimento, reso disponibile prima dell'entrata in vigore del provvedimento del garante.

Entro la fine del corrente anno, d'intesa tra le parti, verrà effettuato un incontro per l'eventuale verifica congiunta della funzionalità del sistema sia in sede di prima applicazione che per la valutazione delle relative eventuali modifiche ritenute necessarie anche con particolare attenzione alla gestione delle segnalazioni.
Saranno comunque effettuati fra le parti incontri di verifica annuale in merito all'applicazione degli accordi in materia.

Per quanto altro non espressamente richiamato nel presente Accordo quadro, si fa rinvio alle prescrizioni del Provvedimento del Garante per la protezione dei dati personali in oggetto e all'accordo quadro del 15.04.2014 .

L'Azienda

Le OO.SS.

DIRCREDITO

UILCA

FISAC CGIL

SINFUB

FIBA CISL

FABI

UGL

Caratteristiche tecniche	Base dati dipartimentale, infrastruttura standard. Prodotto DB standard di mercato.
Ubicazione	CED del Gruppo MPS
Informazioni di base gestite	Per gli accessi puntuali: • Codice ABI dell'azienda • Codice identificativo dell'operatore • Data e ora di esecuzione • Codice della postazione di lavoro utilizzata • Codice operazione attivato • NDG del cliente interessato • Codice rapporto del cliente interessato • Tipologia di operazione (dispositiva, interrogazione) Per gli accessi massivi: • Codice ABI dell'azienda • Codice identificativo dell'operatore • Data e ora di esecuzione • Codice della postazione di lavoro utilizzata • Codice operazione attivato dall'operatore • Parametri della richiesta
Informazioni accessorie	Informazioni connesse al Codice Operatore e al NDG/Rapporto interessato, finalizzate alla rilevazione degli alert.
Modalità di accesso	Riconoscimento ruoli e profili e tracciatura degli accessi secondo gli standard del controllo accessi
Sicurezza fisica	Procedure di backup come da standard di sistema
Termini di conservazione	24 mesi
Periodicità di aggiornamento	Giornaliera
Modalità di alimentazione	1) Selezione delle operazioni bancarie di interesse 2) Acquisizione, completamento e normalizzazione delle informazioni 3) Inserimento dei dati nel log Privacy