Verbale di Accordo

Il giorno 16 settembre 2014, in Arezzo,

tra

la Banca Popolare dell'Etruria e del Lazio

e

le Organizzazioni Sindacali Aziendali
- ✓ DIRCREDITO
- ✓ FABI
- ✓ FIBA CISL
- ✓ FISAC CGIL
- ✓ UILCA

premesso che:

a. Il D.lgs. 30 giugno 2003, n. 196, rubricato *"Codice in materia di protezione di 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;

b. 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,

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

d. L'Abi, con nota del 28/04/2014, chiedeva al Garante la proroga del termine per l'attuazione del Provvedimento al fine di permettere alle Banche di sottoscrivere i necessari accordi aziendali o di Gruppo ai sensi dell'art. 4 della legge n. 300/70;

e. Il Garante, con Provvedimento n. 257/2014 ha accolto la richiesta dell'Abi ed ha prorogato al 30/09/2014 il termine per dare attuazione alle prescrizioni contenute nel Provvedimento n. 192/2011;

f. il Provvedimento - che entrerà in vigore il 30 settembre 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 (Codice in materia dei dati personali), 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;

g. 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*";

h. il Provvedimento si applica a tutti i lavoratori incaricati dall'azienda per i 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;

i. 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*";

j. 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*";

k. 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*";

l. 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*";

m. 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;

n. l'art. 114 del D.lgs 30 giugno 2003, n. 196 stabilisce che "resta fermo quanto disposto dall'art. 4 della legge 20 maggio 1970, n. 300;

o. ABI e le OO.SS. a livello nazionale, considerate le peculiari caratteristiche del provvedimento, in relazione alle previsioni del citato art. 4 l. n. 300/70, nel rispetto delle esigenze di tutela individuale, di quelle aziendali, nonché delle specifiche prerogative sindacali, hanno inteso promuovere il raggiungimento delle correlate intese aziendali, tramite uno specifico Accordo quadro nazionale, finalizzato esclusivamente alle esigenze di adempiere al Provvedimento;

p. In data 15 aprile è stato quindi sottoscritto, tra ABI e le OO.SS., l'accordo quadro nazionale sull'applicazione del Provvedimento del Garante per la protezione dei dati personali del 12/05/2011 n. 192 – che qui si intende integralmente trascritto – che definisce lo schema generale di accordo da utilizzare, a livello aziendale o di gruppo, per la sottoscrizione di intese ex art. 4, comma 2, l. n. 300/70 in specifica attuazione del Provvedimento stesso;

q. le parti si sono quindi incontrate al fine di pervenire ad un accordo in materia, da recepire entro la data prevista del 30/09/2014;

si conviene quanto segue:

1. la premessa forma parte integrante e sostanziale del presente Accordo;
2. Le informazioni riguardanti il trattamento dei dati da parte dell'incaricato, ossia il suo accesso a tali dati (LOG) sono conservate in archivi dedicati presso l'outosourcer esterno Cedacri;
3. I sistemi informativi sono impostati in modo tale che la procedura registra dettagliatamente in appositi file di log, gli accessi - sia dispositivi sia informativi - effettuati dagli incaricati del trattamento sui dati bancari;

   Per ogni accesso effettuato, i file di log conterranno le seguenti informazioni minime:
   - il codice identificativo del soggetto che ha posto in essere l'operazione bancaria;
   - la data e l'ora dell'esecuzione;
   - il codice della postazione di lavoro utilizzata;
   - il codice del cliente interessato dall'operazione;
   - la tipologia di rapporto contrattuale del cliente (es. numero del conto corrente, fido/mutuo, deposito titoli);
4. Nel caso in cui si evidenziasse la necessità di tracciare ulteriori dati rispetto a quelli qui elencati, le integrazioni saranno oggetto di un incontro sindacale di illustrazione a livello aziendale che verrà ripetuto in caso di significative variazioni;
5. I file log relativi alle operazioni sono conservati per un periodo di 24 mesi e possono essere interrogati dalle funzioni di controllo attraverso un sistema di accesso allo strumento,

protetto da specifiche credenziali. Trascorsi i 24 mesi previsti dalla normativa, l'outsourcer provvede ad eliminare i file log archiviati;

6. Come richiesto dal Garante, il sistema di tracciatura definito dall'outsourcer, in cui confluiscono i log relativi a tutti gli applicativi effettuati per gli accessi, consente di attivare specifici alert automatici funzionali all'individuazione di comportamenti anomali o a rischio relativi alle operazioni di inquiry eseguite dagli utenti. La gestione degli alert avviene attraverso un'applicazione che genera dei flussi e alimenta un workflow di gestione delle relative comunicazioni. Le evidenze di alert sono conservate per un periodo di 24 mesi;

7. L'attività di controllo degli alert è demandata, ai sensi del Provvedimento del Garante, "*a unità organizzativa e, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti*";

8. In particolare la Funzione di Compliance provvede ad interrogare l'applicativo per la consultazione (Microstrategy) per la verifica degli alert generati. Una volta effettuate le proprie verifiche, la Funzione di Compliance valuta se chiudere la segnalazione come "falso positivo" o, qualora riscontri anomalie che possano ragionevolmente far configurare comportamenti censurabili, inoltra tale segnalazione alla Funzione di Internal Audit affinché la stessa possa procedere a quanto di propria competenza. Inoltre, la Funzione di Compliance, valuta e verifica nel continuo la parametrizzazione degli alert adottati/adottabili segnalando, previa condivisione con la Funzione di Internal Audit, al Dipartimento Organizzazione e IT le variazioni da apportare. Con cadenza almeno semestrale, effettua inoltre verifiche a posteriori e a campione sugli accessi ai dati effettuati dagli incaricati. A seguito delle segnalazioni pervenute, il Dipartimento Organizzazione e IT provvederà ad interessare l'outsourcer per apportare le modifiche richieste;

9. In data odierna la funzione di Compliance è intervenuta per illustrare alle OO.SS. i principi generali che determineranno l'attivazione degli alert e che saranno formulati nell'allegato tecnico alla circolare: entro sei mesi dall'entrata in vigore del Provvedimento, Le parti si incontreranno per dare un'informativa sulle modalità delle indagini a campione e sui risultati ottenuti nella produzione dei suddetti alert;

10. Qualora, nel corso delle analisi di cui sopra, dovessero emergere profili di particolare gravità, verrà inviata una comunicazione al Dipendente interessato. In tal caso, il dipendente potrà essere sentito, anche su sua richiesta, con l'assistenza di un rappresentante sindacale dell'Organizzazione a cui aderisce o conferisce mandato;

11. 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;

12. L'esito dell'attività di controllo è richiamato nella relazione annuale sull'attività svolta dalla funzione di Compliance, quale informativa verso gli Organi Sociali;

13. La Funzione di Internal Audit effettua con cadenza periodica (almeno annuale) un'attività di controllo e verifica sulla gestione della tracciatura e della conservazione delle registrazioni, in modo da verificare la rispondenza del sistema dei controlli con le misure organizzative, tecniche e di sicurezza riguardanti i dati bancari, nei modi e nei tempi previsti dalla normativa di cui al Provvedimento del Garante;

14. Il Personale viene informato delle procedure adottate ai sensi delle precedenti sezioni 1 e 2 e dei connessi adempimenti tramite le consuete modalità di informativa aziendale;

15. L'utilizzo degli strumenti regolati dal presente Accordo è finalizzato esclusivamente ad adempiere alle necessità illustrate in premessa, con particolare riferimento agli adempimenti previsti dai Provvedimenti del Garante citati nell'Accordo stesso. Viene pertanto esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dei Dipendenti, escludendo altresì espressamente che l'uso dei dati possa avvenire per scopi relativi alla sfera soggettiva del Dipendente interessato;

16. Per quanto non espressamente richiamato nel presente Accordo, si fa rinvio alle correlate prescrizioni dell'Accordo Quadro Nazionale 15.04.2014 e del Provvedimento del Garante per la protezione dei dati personali.

Letto, confermato e sottoscritto.

BPEL

LE OO.SS

DIRCREDITO

FIBA CISL

UILCA

FISAC

FABI