**ACCORDO EX ART. 4, COMMA 2, L. 20.5.1970 N°300 SULL'APPLICAZIONE DEL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 12 MAGGIO 2011, N. 192**

Il giorno 11 luglio 2014, in Milano,

tra

ICBPI S.p.A., anche in qualità di Capogruppo del Gruppo ICBPI, rappresentata dal Servizio Risorse Umane

e

DIRCREDITO-FD
FABI
FIBA-CISL
FISAC-CGIL
SINFUB

Premesso che:

a) il D.Lgs. 30 giugno 2003, n. 196, rubricato "Codice in materia di protezione dei dati personali" (di seguito il "Codice") 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 (di seguito "il Garante");
b) il Garante 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 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" (di seguito il "Provvedimento"); in data 18 luglio 2013 e 22 maggio 2014 lo stesso Garante ha emanato rispettivamente i Provvedimenti n. 357 e n. 257, e ne ha differito il termine previsto per l'entrata in vigore;
d) 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 prescrizioni, ai sensi dell'art. 154, comma 1, lett. c), 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;

e) 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";

f) 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";

g) 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";

h) 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";

i) 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";

j) 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;

k) 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";

l) 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";

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

n) le misure del Provvedimento "debbono essere osservate pure dalle Società che operano in outsourcing – anche quando non appartengono al gruppo bancario – allorchè 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 ";

o) ABI e le OO.SS. a livello nazionale, considerate le peculiari caratteristiche del Provvedimento, in relazione alle previsioni del citato art. 4 L. 300/1970, 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 2014 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 maggio 2011, n. 192" - che qui si dà per 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. 300/1970 in specifica attuazione del Provvedimento stesso;

q) tale Accordo Quadro stabilisce, infatti, che, 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 l'organizzazione del lavoro e della produzione, con riferimento, tra l'altro, alla "introduzione di nuove tecnologie", i predetti accordi possono essere stipulati con gli organismi sindacali aziendali di cui all'art. 24 del CCNL 19 gennaio 2012 o, se condiviso tra le Parti, con la delegazione di Gruppo di cui all'art. 25 dell'Accordo in materia di libertà sindacali del 7 luglio 2010, considerata la necessaria uniformità ed il carattere eccezionale degli adempimenti connessi all'attuazione del Provvedimento;

r) ai fini di cui sopra il confronto a livello aziendale o di Gruppo è finalizzato a verificare la coerenza delle proposte dell'Azienda con le vigenti disposizioni in materia ed il predetto Accordo Quadro ed a stipulare i conseguenti accordi ex art. 4, comma 2, L. n. 300 del 1970, a valere per gli specifici e connessi effetti entro la predetta data del 30 settembre 2014;

s) le parti hanno quindi condiviso di sottoscrivere l'accordo ex art. 4 L. 300/70 con le RSA delle unità produttive di ICBPI, che rientrano nell'ambito di applicazione del Provvedimento;

t) l'Azienda ha illustrato alle predette Rappresentanze Sindacali Aziendali di ICBPI, nel corso di un apposito incontro, le caratteristiche e il funzionamento degli strumenti informatici predisposti al fine di adeguare i propri sistemi alle prescrizioni del Provvedimento e le stesse sono informate in ordine alla unità organizzativa cui è affidato il trattamento dei dati bancari dei clienti nonché sulle modalità di indagine a campione,

si conviene quanto segue:

1. la premessa forma parte integrante e sostanziale del presente Accordo;
2. le soluzioni informatiche adottate sono destinate al controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database, ai sensi di quanto prescritto dal Garante con il Provvedimento. A tal fine è stato adottato un applicativo denominato "Splunk" per la storicizzazione dei dati e per l'implementazione e generazione di alert volti a rilevare accessi anomali ai sistemi informativi tramite le applicazioni che, nell'ambito dell'Azienda, a fronte dell'esecuzione di funzionalità operative, rendono disponibili dati bancari delle persone fisiche;
3. le specifiche tecniche e organizzative apprestate - comunicate alle rsa e riportate nel presente accordo - e le eventuali modifiche formano parte integrante dell'accordo aziendale o di gruppo e sono oggetto di un incontro sindacale di illustrazione a livello aziendale, che verrà ripetuto in caso di significative variazioni;
4. a seguito di analisi effettuate dal Servizio Sistemi Informativi, sono state individuate una serie di applicazioni rilevanti ai fini della presente normativa all'interno di ICBPI, elencate nell'Allegato 1, parte integrante del presente accordo.

   Tali applicazioni saranno oggetto di registrazione dettagliata, in appositi files di log, al fine di tracciare le informazioni riferite alle operazioni bancarie, effettuate sui dati bancari dagli incaricati del trattamento utenti delle applicazioni in perimetro. In particolare, i files di log registreranno, per ogni operazione di accesso ai dati bancari effettuata da un incaricato, le seguenti informazioni:

   - matricola identificativa dell'utente

- data ed ora dell'operazione
- il codice della postazione di lavoro utilizzata
- il codice Identificativo del cliente (ad es. NDG) 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.

Nel caso in cui si evidenziasse la necessità di tracciare ulteriori dati rispetto a quelli qui elencati, le integrazioni formeranno parte integrante dell'accordo aziendale o di gruppo e sono oggetto di un incontro sindacale di illustrazione a livello aziendale, che verrà ripetuto in caso di significative variazioni;

5. i log di tracciamento delle operazione 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;
6. come espressamente richiesto dal Garante, sono attivati specifici alert finalizzati ad individuare comportamenti anomali o a rischio relativi alle operazione di inquiry eseguite dagli incaricati del trattamento. In particolare, viene monitorato l'accesso ai dati di un singolo cliente o di più clienti da parte di un singolo operatore, in base al superamento di soglie specifiche applicate alle seguenti variabili:
   - numero di accessi al singolo dato
   - fascia oraria di accesso al dato;

7. ai sensi del Provvedimento e successive integrazioni:
   a. 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;
   b. l'attività di controllo e di verifica degli alert è demandata al Servizio Audit, che opera attraverso cinque incaricati della struttura. Eventuali future modifiche o integrazioni saranno previamente comunicate alle rsa, fermo restando che le attività di controllo dovranno essere comunque affidate a personale diverso rispetto a quello abilitato al trattamento dei dati bancari dei clienti;
   c. i controlli comprendono anche verifiche a posteriori, a campione o 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;

d. 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;

8. 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 tutto il personale attraverso specifici ed opportuni strumenti. Inoltre, nell'ambito di quanto previsto dall'art. 72 del CCNL 19 gennaio 2012, potranno essere previste, ove necessario, specifiche attività formative retribuite;
9. in sede aziendale saranno possibili, d'intesa tra le Parti, incontri di verifica annuale in merito all'applicazione del presente accordo.

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

Per Istituto Centrale delle Banche Popolari Italiane S.p.A.

Per le OO.SS.

**Allegato 1**

**GESTIONE DEGLI ALERT (PROVVEDIMENTO AUTORITA' GARANTE PRIVACY PER IL TRACCIAMENTO DELLE OPERAZIONI BANCARIE – PERIMETRO APPLICATIVO**

- ABC
- W2PEX
- Anacomp
- RMT Proteso
- GE49
- Gianos 3D

Milano, 11 luglio 2014