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

Il 15 aprile 2014

tra

ABI

e

- DIRCREDITO-FD
- 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. con il verbale di accordo del 20 dicembre 2013 le Parti stipulanti hanno assunto l'impegno di stipulare, entro il 31 marzo 2014, un Accordo quadro per l'attuazione nel settore del credito dei richiamati Provvedimenti del Garante;

5. 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;

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

7. 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";

8. 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";

9. 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";

10. 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";

11. 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;

12. 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";

13. 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";

14. il Provvedimento definisce "un quadro unitario di misure necessarie e opportune" per tutte le banche e i gruppi bancari di cui al punto 5 che precede;

15. 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";

16. le Parti, considerate le peculiari caratteristiche del Provvedimento, intendono promuovere il raggiungimento delle correlate intese aziendali, tramite uno specifico Accordo quadro nazionale, finalizzato esclusivamente alle esigenze di adempiere al succitato Provvedimento del Garante,

tutto ciò premesso, le Parti

ABI

DIRCREDITO-FD FABI FIBA-CISL FISAC-CGIL SINFUB UGL CREDITO UILCA

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 quadro;
- il presente Accordo quadro definisce lo "schema generale di accordo" da utilizzare per la stipulazione di intese ex art. 4, comma 2, l. n. 300 del 1970 in specifica attuazione del Provvedimento in oggetto;
- 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 del Garante;
- ai fini di cui sopra il confronto a livello aziendale o di gruppo è finalizzato a verificare la coerenza delle proposte dell'impresa con le vigenti disposizioni in materia ed il presente Accordo quadro ed a stipulare i conseguenti accordi ex art. 4, comma 2, l. n. 300 del 1970 entro il mese di aprile 2014, a valere ad ogni conseguente effetto dalla predetta data del 3 giugno 2014;

SCHEMA GENERALE DI ACCORDO EX ART. 4 L. N. 300 DEL 1970

Le banche ed i gruppi bancari e le società di cui in premessa adottano 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 del cliente a cui si riferisce l'operazione effettuata". Gli ulteriori dati funzionali alla realizzazione delle finalità previste dal Provvedimento saranno oggetto di informativa a livello aziendale o di gruppo.

"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.

Le specifiche tecniche e organizzative apprestate 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.

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. Le relative caratteristiche sono specificate nell'accordo aziendale o di gruppo.

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 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;

- "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".

I lavoratori incaricati sono informati delle procedure adottate e dei connessi adempimenti tramite apposita informativa (art. 13 d.lgs. n. 196 del 2003), che deve essere portata a conoscenza di tutti i lavoratori attraverso specifici ed opportuni strumenti. Inoltre, nell'ambito di quanto previsto dall'art. 72 del ccnl 19 gennaio 2012, possono svolgersi, ove necessario, specifiche attività formative retribuite.

In sede aziendale saranno possibili, d'intesa fra le parti, incontri di verifica annuale in merito all'applicazione degli accordi in materia.

In sede aziendale o di gruppo vengono fornite informazioni agli Organismi sindacali 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 quadro, si fa rinvio alle prescrizioni del Provvedimento del Garante per la protezione dei dati personali in oggetto.