In data odierna, 23 settembre 2014, presso la sede di Unipol Banca S.p.A. in Bologna,

tra

UNIPOL BANCA S.p.A.

e

le delegazioni sindacali:

DIRCREDITO	rappresentata dai sigg.ri	Alberto Forlai e Marco Militerno
FABI	rappresentata dai sigg.ri	Adriano Di Martino e Mattia Pari;
FIBA/CISL	rappresentata dai sigg.ri	Vincenzo Montevago e Alessandro Rivano;
FISAC/CGIL	rappresentata dai sigg.ri	Fabio Naldi e Paolo Riga;
U.G.L.	rappresentata dai sigg.ri	Luigi Bernabei;
UIL C.A.	rappresentata dai sigg.ri	Claudio Migliorini e Marco Aversa.

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 al 3 giugno 2014; in data 22 maggio 2014, lo stesso Garante ha emanato il Provvedimento n. 257 e ne ha differito il termine previsto per l'entrata in vigore al 30 settembre 2014;
- il Provvedimento è finalizzato a "garantire il rispetto dei principi in materia di protezione dei dati personali ai sensi del relativo 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;
- in data 15 aprile 2014 è stato 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 e che definisce lo schema generale di accordo da utilizzare per la sottoscrizione di intese ex art. 4, comma 2, L. n. 300/1970 in specifica attuazione del Provvedimento in oggetto;
- tale accordo quadro stabilisce che il confronto finalizzato a verificare la coerenza di quanto proposto dall'impresa con le vigenti disposizioni in materia possa essere svolto a livello

aziendale o di gruppo anziché a livello di Rappresentanze Sindacali Aziendali come stabilito dal citato art. 4 L. n. 300/1970;

- le Parti si sono quindi incontrate al fine di pervenire ad un accordo in materia;

Considerato che:

Il Provvedimento riguarda le operazioni relative ai clienti degli istituti bancari di cui al quarto alinea delle premesse, "sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, c.d. *inquiry*".

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".

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".

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;

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".

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.

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".
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".

Il Provvedimento definisce "un quadro unitario di misure necessarie e opportune" per tutte le banche e i gruppi bancari soggetti alla disciplina.

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".

Tutto ciò premesso e considerato, le Parti convengono quanto segue:

Le premesse formano parte integrante e sostanziale del presente Accordo.

Viene data attuazione al sopra richiamato 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.

La Banca adotta idonee soluzioni informatiche per il controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui vari database, ai sensi di quanto prescritto dal Garante per la protezione dei dati personali con il Provvedimento n.192 del 12 maggio 2011 e n. 357 del 18 luglio 2013.

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 tracceranno, per ogni operazione di accesso ai dati bancari effettuata da un incaricato, 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 *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, riportate negli allegati 1 e 2, formano parte integrante del presente accordo e le eventuali future modifiche saranno oggetto di confronto con le Organizzazioni Sindacali e costituiranno parte integrante del presente accordo.

Come espressamente richiesto dal Garante sono attivati "specifici *alert*" finalizzati ad individuare comportamenti anomali o a rischio relativi alle operazioni di *inquiry* eseguite dagli incaricati del trattamento, le cui caratteristiche sono state illustrate alle Organizzazioni Sindacali e sono specificate nell'allegato 2.

Ai sensi del Provvedimento n. 192 del 12 maggio 2011 e successive integrazioni:
- "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 alle unità di Compliance e Audit;
- "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 tempo per tempo incaricati saranno destinatari di apposita informativa in merito alle procedure adottate ed ai connessi adempimenti ai sensi dell'art.13 del d.lgs. n.196 del 30 giugno 2003; tale informativa viene portata a conoscenza di tutti i lavoratori. Inoltre, nell'ambito di quanto previsto dall'art. 72 del ccnl 19 gennaio 2012, possono svolgersi, ove necessario, specifiche attività formative retribuite.

In particolare, nella fase di prima attuazione del Provvedimento:
- viene pubblicata apposita circolare con informativa sul Provvedimento e sugli strumenti utilizzati;
- viene messo a disposizione di tutto il personale un modulo formativo a distanza a fruizione obbligatoria retribuita riguardante le prescrizioni del Provvedimento del Garante.

In sede aziendale saranno effettuati, a richiesta delle Organizzazioni Sindacali, incontri di verifica semestrale in merito all'applicazione degli accordi in materia con riferimento al numero di alert generati e agli esiti dei controlli. Un primo incontro di verifica sull'attuazione della fase di avvio del Provvedimento verrà effettuato entro il 31 marzo 2015.

In sede aziendale vengono fornite informazioni agli Organismi sindacali in ordine alle 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 dell'Accordo Quadro di settore del 15 aprile 2014 e del Provvedimento del Garante per la protezione dei dati personali n.192 del 12 maggio 2011 e n. 357 del 18 luglio 2013.

UNIPOL BANCA S.p.A.

DIRCREDITO **FABI** **FIBA/CISL** **FISAC/CGIL** **U.G.L.** **UIL C.A.**

Tracciatura delle operazioni bancarie

SCHEDA ESPLICATIVA

Dettagli tecnici base dati

Allegato n. 1 – Appendice all'accordo del 23 settembre 2014 (parte 1 di 2)

Caratteristiche tecniche	Data Base Oracle
Ubicazione	Cedacri
Termine di conservazione	24 mesi
Modalità accesso	Per garantire l'accesso solo alle persone autorizzate delle funzioni di Compliance e Audit, il Data Base del garante è stato posizionato nella rete interna di Cedacri con credenziali controllate attraverso un firewall e accessi all'ambiente Oracle tramite utenze con ruoli definiti secondo il principio del "minimo privilegio". L'accesso da parte di personale della Banca è eseguito solo tramite l'interfaccia di consultazione, che prevede un'autenticazione con username e password personali.

Tracciatura delle operazioni bancarie

SCHEDA ESPLICATIVA

Descrizione del processo e caratteristiche tecniche delle elaborazioni

Allegato n. 1 – Appendice all'accordo del 23 settembre 2014 (parte 2 di 2)

Ai fini della tracciatura delle operazioni bancarie come richiesto dal Garante per la protezione dei dati personali:

1.- per tutte le operazioni bancarie eseguite sui sistemi si verifica se sono da tracciare secondo le disposizioni del Provvedimento, ossia se trattano dati bancari di clienti soggetti alla normativa privacy vigente (persone fisiche come classificate in anagrafe clienti e ditte individuali);

2.- le operazioni individuate in ambito al punto precedente sono registrate dalle singole procedure nelle basi dati, tutte in infrastruttura standard. Le informazioni registrate sono esclusivamente le informazioni richieste dal provvedimento, ossia:

- 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 (es. numero del conto corrente, fido/mutuo, deposito titoli).

3.- giornalmente le operazioni vengono inviate in modo automatico, mediante infrastruttura di trasferimento file standard, ad una unica base dati centralizzata, che le raccoglie per i 24 mesi previsti dal provvedimento. Tutta l'attività di estrazione, invio e ricezione è automatizzata;

4.- le operazioni ricevute sono inserite nella base dati centralizzata dove vengono mantenute per 24 mesi. L'infrastruttura della base dati è dedicata e in infrastruttura standard. Le strutture tecnologiche utilizzate sono standard e di mercato.

Come previsto dal Provvedimento del Garante n. 357 del 18 luglio 2013, nel caso in cui l'operazione non sia indirizzata ad un identificativo di cliente o rapporto specifico (ricerche massive) le informazioni registrate sono:

- i dati relativi all'incaricato che ha eseguito la *query*;
- la data e l'ora;
- il dettaglio della relativa richiesta.

5.- reporting: sulla base dati è prevista la creazione di report con interfaccia standard Microstrategy, il cui accesso sarà consentito alle funzioni di Compliance e Audit.

Sistema di Alert

Allegato n. 2 – Appendice all'accordo del 23 settembre 2014

È stato previsto un set standard di regole base per la generazione degli alert, come di seguito identificate:

- numero di accessi ai dati del singolo cliente, effettuati nella giornata dallo stesso incaricato, superiore a N;
- numero di accessi ai dati del singolo cliente, effettuati nella giornata da più incaricati, superiore a N;
- numero di accessi ai dati del singolo cliente, effettuati nell'unità di tempo dallo stesso incaricato, superiore a N;
- numero di accessi ai dati del singolo cliente, effettuati nell'unità di tempo da più incaricati, superiore a N;
- numero di accessi su rapporti in circolarità, effettuati nella giornata dallo stesso incaricato, superiore a N;
- numero di accessi su rapporti in circolarità, effettuati nell'unità di tempo dallo stesso incaricato, superiore a N.