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 26 maggio 2014, in Milano,

tra

la Deutsche Bank S.p.A., anche in qualità di Capogruppo del Gruppo Bancario Deutsche Bank in Italia (di seguito la "Banca"), rappresentata dai Sigg. F. Zambruno, F. Ponti, M. Gurgoglione e M. Cavallaro

e

le Delegazioni Sindacali di Gruppo delle OO.SS.

- FABI rappresentata dai Sigg. S. Caldara, M. Belfiore, E. Camisasca, E. Campi, M. Panigada, T. Guepa e M. Galli
- FIBA-CISL rappresentata dai Sigg. M. Gemelli, D. Iodice, M. Cazzamalli, A. Luppi, M. Marino, M. Pontiggia e S. Toso
- FISAC-CGIL rappresentata dai Sigg. C. Cornelli, M. Bordini, L. Santosuosso, A. Pozzi, R. Salzano, M. Colombo e E. Bovero
- UILCA rappresentata dai Sigg. R. De Giovanni, S. Bertelli, R. Morra, C. Napolitano, S. Cenacchi, R. Della Noce e S. Martorelli

(di seguito le "OO.SS.)

Premesso che:

a) 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 (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, lo stesso Garante ha emanato il Provvedimento n. 357 e ne ha differito il termine previsto per l'entrata in vigore;

d) 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 relativo 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 prevede espressamente che "restano salve le norme del Codice in materia di trasferimento dei dati all'estero da parte dei titolari del trattamento. In relazione a tale aspetto l'Autorità si riserva, qualora se ne dovesse ravvisare la necessità, di intervenire con un successivo provvedimento".

m) 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";

n) 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;

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'impresa 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 dalla predetta data del 3 giugno 2014;

s) le parti hanno quindi condiviso di sottoscrivere l'accordo ex art. 4 L. 300/70 con le Delegazioni di gruppo, valevole per tutte le società del gruppo rientranti nell'ambito di applicazione del Provvedimento;

t) La Banca ha illustrato alle Delegazioni Sindacali di gruppo, nel corso di apposito incontro, le caratteristiche e il funzionamento degli strumenti informatici predisposti al fine di adeguare i propri sistemi alle prescrizioni del Provvedimento,

si conviene quanto segue:

1. La premessa forma parte integrante e sostanziale del presente Accordo che si applica a tutte le unità produttive delle aziende facenti parte del Gruppo Deutsche Bank S.p.A. presenti in Italia e specificatamente a:
   - Deutsche Bank SpA
   - DB Mutui SpA
   - Finanza & Futuro Banca SpA
   - Fiduciaria S. Andrea srl
   - DB Consorzio Scarl
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 realizzato un "repository" centrale (denominato "Privacy PG2") per la storicizzazione dei dati e per l'implementazione di alert volti a rilevare accessi anomali ai sistemi informativi tramite le applicazioni che, nell'ambito delle aziende del Gruppo, a fronte dell'esecuzione di funzionalità interattive, rendono disponibili dati bancari delle persone fisiche.

FABI FIBA UILCA

3. Le specifiche tecniche del sistema sono riportate nel documento allegato e formano parte integrante del presente accordo. Le eventuali future modifiche formeranno oggetto di specifica informativa alle Delegazioni sindacali firmatarie del presente accordo nel corso di apposito incontro, nell'ambito del quale le parti valuteranno l'eventuale necessità di modificare o integrare l'accordo stesso.
4. 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:
   - Matricola identificativa dell'utente
   - data ed ora dell'operazione
   - il codice della postazione di lavoro utilizzata
   - il codice Identificativo del cliente (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
   - Tipologia di operazione
   - Codice Operazione
   - Gruppo Applicativo (dato previsto solo per alcune applicazioni)
   - Criteri di selezione impostati (il contenuto è rappresentato dai filtri –dove applicabili- impiegati dall'utente nella selezione dei clienti)

   Nel caso in cui si evidenziasse la necessità di tracciare ulteriori dati rispetto a quelli qui elencati e contenuti nell'allegato, le integrazioni saranno oggetto di specifica informativa alle Delegazioni firmatarie del presente accordo, nel corso di apposito incontro, nell'ambito del quale le parti valuteranno l'eventuale necessità di modificare o integrare l'accordo stesso.
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, come specificato più in dettaglio nell'allegato.
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 è demandata all'unità organizzativa ORM del gruppo DB S.p.A., che opera attraverso l'utilizzo di n. 4 utenze ed è soggetta al controllo della funzione Audit del Gruppo DB S.p.A. Eventuali future modifiche o integrazioni saranno previamente comunicate alle OO.SS, fermo restando che 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, su campione scelto casualmente, 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, compresa la pubblicazione in Normativa Online. 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 effettuati, a richiesta delle OO.SS., incontri di verifica annuale in merito all'applicazione del presente accordo ad esito delle attività di cui al punto 7 che precede, anche con riferimento al numero di alert generati nell'ambito della singola azienda e all'esito degli stessi. Le OO.SS. potranno richiedere trimestralmente la disponibilità dei log delle attività condotte da parte delle funzioni abilitate a norma del punto 7 b. che precede.
10. Entro quattro mesi dall'entrata in vigore del Provvedimento la Banca fornirà alle OO.SS. un'informativa sulle modalità delle indagini a campione e sui risultati ottenuti nella produzione degli alert in base agli indicatori riportati nell'allegato.
11. Il presente accordo viene sottoscritto tra le parti, nel presupposto dell'eccezionalità del Provvedimento, esclusivamente con la finalità e per l'effetto di dar corso agli adempimenti previsti dal Provvedimento stesso, restando pertanto esclusa qualsiasi finalità di controllo a distanza di tempo e di luogo, diretto o indiretto, sulla qualità e/o quantità dell'attività

FABI FIBA UILCA

lavorativa svolta da ogni singolo utente. Pertanto l'accesso al sistema di cui al presente accordo (Privacy PG2) da parte delle competenti funzioni aziendali a norma del punto 7 che precede, non potrà avvenire al di fuori dei casi espressamente qui previsti e, segnatamente:

- a fronte di richieste delle autorità competenti ovvero della clientela
- per effettuare i controlli previsti al punto 7 c. che precede

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

DICHIARAZIONE DELLE OO.SS.

Con riferimento a punto s) della premessa, Le OO.SS. dichiarano che il presente accordo viene eccezionalmente sottoscritto dalle Delegazioni di gruppo rispetto alla competenza prevista dall'art. 4 della L. 300/70.

DEUTSCHE BANK S.p.A.

FISAC

UILCA

FIBA

FABI

ALLEGATO
all'accordo ex art. 4,co 2, L. 20.5.1970 n°300 sull'applicazione del provvedimento del Garante per la protezione dei dati personali del 13.5.2011, n. 192

1. PREMESSA

Il presente documento descrive gli interventi previsti dal Gruppo DB S.p.A Italia al fine di adeguarsi alle nuove norme imposte dal Provvedimento n. 192 del 12 maggio 2011 (in seguito chiamato "Provvedimento") emesso dal Garante per la Protezione dei Dati Personali nei confronti di Banche o Gruppi Bancari stabiliti sul territorio nazionale, intitolato "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie".

In data 18 luglio 2013 il Garante ha prorogato l'entrata in vigore del provvedimento al 3 giugno 2014 e ha fornito alcuni chiarimenti ai quesiti posti dal gruppo di lavoro dell'ABILAb.

2. ELEMENTI IN SCOPE AL PROVVEDIMENTO

La pertinenza del progetto e' quella di definire esclusivamente gli interventi sui sistemi informativi delle Legal Entitiy del Gruppo operanti in Italia e, in particolare:

- Gruppo DB S.p.A
- DB Mutui SpA
- Finanza & Futuro Banca SpA
- Fiduciaria S. Andrea srl
- DB Consorzio Scarl

necessari a soddisfare i requisiti del Provvedimento.

Il Progetto prende in esame le applicazioni definite all'interno del parco applicativo che, a fronte dell'esecuzione di funzionalità interattive, rendono disponibili dati bancari delle persone fisiche.

In particolare sono considerate nel perimetro le applicazioni che:

- *consentono il trattamento di dati delle persone fisiche*
- *consentono il trattamento di dati bancari*
- *offrono funzioni interattive agli utenti incaricati del trattamento*
- *consentono l'accesso in interrogazione a dati della clientela, anche in forma di liste, quando l'output mostri un riferimento esplicito al singolo cliente*

Il provvedimento sarà attuato attraverso la progettazione e sviluppo di un repository centrale **(Privacy PG2)** che consenta di ottemperare alla richiesta del Garante riguardo alla storicizzazione dei dati, all'implementazione di alert volti a rilevare accessi anomali ai sistemi informativi.

2.1 Struttura del Modello

Il gruppo Gruppo DB S.p.A garantirà l'adeguamento al provvedimento Garante Privacy 192/2011 attraverso l'implementazione di un modello organizzativo e l'adozione dei processi che ne discenderanno, e si avvarrà di soluzioni informatiche al fine di collezionare i dati relativi al provvedimento ed alla loro analisi.

Le legal entity in scope al provvedimento adotteranno lo stesso modello di lavoro sia in termini di processi che in termini di soluzioni informatiche da adottare.

L'attuazione delle disposizioni del provvedimento è garantita dalla realizzazione di una soluzione (Privacy PG2) che al contempo consente di:

- Raccogliere le informazioni provenienti dalle applicazioni usate dagli utenti,
- Storicizzare le informazioni raccolte nei termini indicati dal Garante
- Consentire l'analisi dei dati raccolti, sia per rispondere ad eventuali richieste del garante che del cliente e per la definizione degli alert,

- Implementare i sistemi di alerting richiesti dal Garante atti al monitoraggio dei comportamenti degli utenti

La disponibilità dei dati in Privacy PG2 è riservata alle utenze dell'applicazione designate dalla banca stessa (ORM).

2.2 *Il Sistema di Tracciamento*

I dati richiesti dal provvedimento sono raccolti durante l'uso delle applicazioni stesse e poi estratti sotto forma di log. L'abilitazione dell'applicazione alla raccolta dei dati avviene attraverso un adeguamento software.

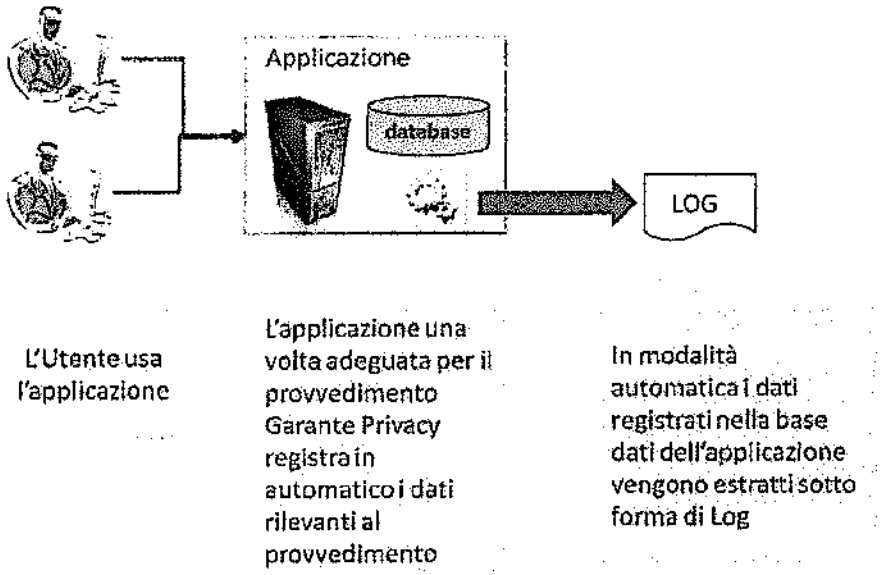

Figura 1 Logica di creazione del Log privacy

Le applicazioni identificate come in perimetro per il provvedimento Privacy, devono essere sottoposte ad un processo di adeguamento al fine di raccogliere i dati richiesti dal Garante della Privacy.

I dati raccolti dall'applicazione durante il suo uso sono relativi alle operazioni bancarie (di tipo interrogativo e dispositivo) effettuate sui dati bancari da parte degli utenti.

I dati raccolti nei Log sono i seguenti:

- Matricola identificativa dell'utente
- Data ed Ora dell'operazione
- Codice Postazione dell'utente
- Identificativo del cliente (NDG)
- Tipo di Rapporto del cliente
- Codice del Rapporto del cliente
- Tipologia di operazione
- Codice Operazione
- Gruppo Applicativo dell'utente (dato previsto solo per alcune applicazioni)
- Criteri di selezione impostati dall'utente (il contenuto è rappresentato dai filtri -dove applicabili- impiegati dall'utente nella selezione dei clienti)

FABI FABI

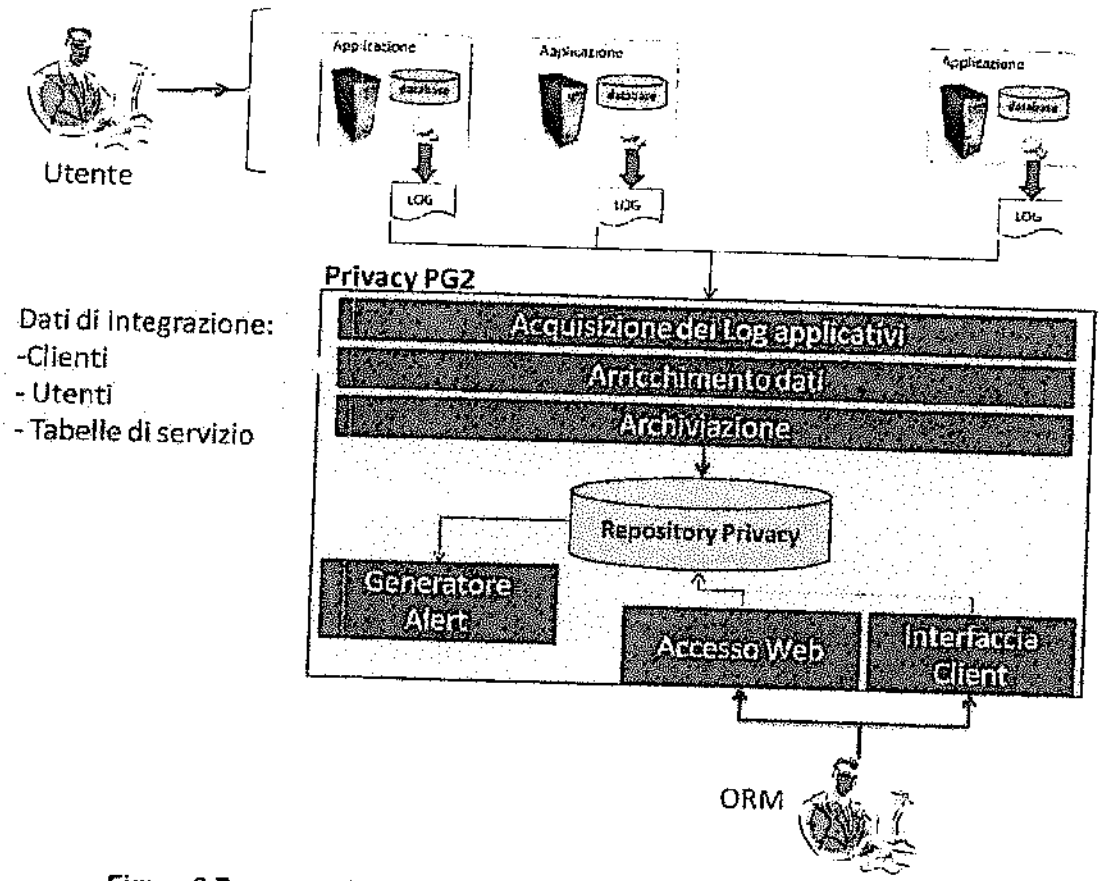

Figura 2 Processo di Acquisizione Log dal sottosistema Privacy PG2

Tutte le applicazioni in scope inviano i Log generati alla soluzione Privacy (Privacy PG2) adottata da Gruppo DB S.p.A, l'invio generalmente (salvo eventuali eccezioni) avviene con cadenza giornaliera (a fine giornata il log viene generato e trasmesso a Privacy PG2).

I dati ricevuti subiscono i seguenti processi automatici:

- Validazione ed acquisizione nell'archivio,
- Completamento con l'ausilio di dati di arricchimento sia relativi ai Clienti che relativi all'utente (società di appartenenza e profilo/ruolo utente se non presente nel log),
- Memorizzazione nel repository della base dati,
- Impiegati nella generazione di alert automatici sulla base di regole stabilite.

Le funzionalità di Privacy PG2 sono disponibili solo alle utenze abilitate (quattro utenti) , l'accesso ai dati dell'applicazione è consentito all'unità ORM per individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati al trattamento. Le modalità operative previste per analizzare i dati raccolti sono le seguenti:

- Accesso tramite interfaccia Web: consente all'utente abilitato di accedere alla consultazione e gestione degli Alert, nonché alla reportistica standard disponibile,
- Accesso tramite Interfaccia Client: consente all'utente abilitato di analizzare accessi anomali e abusivi ai sistemi informativi nonché rispondere alle interrogazioni provenienti dal Garante Privacy e/o alle domande provenienti dal cliente.

I dati raccolti in Privacy PG2 saranno storicizzati per un periodo di 24 mesi.

L'infrastruttura impiegata di Privacy PG2 è nelle server farm di DB ed in particolare:

- Server che ospitano l'applicazione: Oberursel / Eshborn / Fancoforte
- Repository Privacy: Oberursell / Eshborn

3. LE RICHIESTE DEL GARANTE E LA SOLUZIONE DEUTSCHE BANK

In relazione a quanto prescritto dal Garante della Privacy come Misure necessarie Deutsche Bank ha posto in essere le seguenti soluzioni:

A) Tracciamento delle operazioni

Richiesta nel provvedimento del garante

Devono essere adottate idonee soluzioni informatiche per il controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui 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 impiegati dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente.

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

Soluzione DB.

L'approccio di Deutsche Bank è stato quello di

- Definizione di requisiti per tracciatura
- Identificazione del parco applicativo da adeguare
- Identificazione delle funzionalità da adeguare per il tracciamento delle informazioni richieste
- Creazione di un tracciato che contenga tutte le informazioni minime richieste dal Garante

B) Conservazione dei log di tracciamento delle operazioni.

Richiesta nel provvedimento del garante

Il periodo di conservazione dei file di log delle operazioni di inquiry non deve essere inferiore a 24 mesi dalla data di registrazione dell'operazione.

Soluzione DB.

E' stata approntata una soluzione (Privacy PG2) in grado di acquisire automaticamente i flussi provenienti dalle applicazioni alimentanti.
Questa nuova applicazione rispetta tutti gli standard IT di Deutsche Bank secondo i principi di riservatezza basati su profili nell'assegnazione delle facoltà di accesso (soggetta a revisione periodica) agli utenti dell'applicazione e secondo i principi di accountability sulle attività degli utenti e sulle attività degli operatori di controllo è inoltre prevista una segregazione logica per Legal Entity.
L'accesso alle funzioni applicative è gestito dall'U.O. ORM, quale *owner* dei dati, come previsto dalle specifiche policy di sicurezza di Deutsche Bank.

E' stata prevista la conservazione dei dati nel Sistema Privacy per 24 mesi, con un processo mensile di svecchiamento dei log dall'archivio con tracciatura delle azioni realizzate.

FABI FIBA UILCA

C) Implementazione di alert.

Richiesta nel provvedimento del garante

- *Deve essere prefigurata da parte delle banche l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry*
- *Negli strumenti di business intelligence devono confluire i log relativi a tutti gli applicativi utilizzati per gli accessi.*

Soluzione DB.

Come specificamente richiesto dal Garante, sono stati predisposti appositi alert con il fine di individuare *comportamenti anomali o a rischio*, sulla base di specifiche regole di alert ossia:

- Interrogazioni effettuate fuori dalla fascia oraria operativa della struttura di appartenenza (regola applicata alle unità di Direzione Generale, di supporto alla rete e alla rete sportelli);
- Interrogazioni effettuate in giornate non lavorative della struttura di appartenenza (regola applicata alle unità di Direzione Generale, di supporto alla rete e alla rete sportelli);
- Interrogazioni su rapporti non radicati/gestiti rispettivamente presso o dalla struttura organizzativa di appartenenza dell'utente (regola applicata alle unità di Direzione Generale, di supporto alla rete e alla rete sportelli);
- Frequenza di interrogazioni in relazione alla tipologia del rapporto (regola applicata alle unità di Direzione Generale, di supporto alla rete e alla rete sportelli).

L'applicazione Privacy PG2 effettua i controlli sui dati ricevuti, generando una segnalazione di anomalia (alert) nel caso in cui siano superate specifiche soglie stabilite, costituite da un numero predeterminato, oltre il quale le *inquiry* sono presunte come anomale. Le regole di alert sono tarate in funzione dei diversi profili degli utenti.

*D) **Audit interno di controllo–Rapporti periodici.***

Richiesta nel provvedimento del garante

i. La gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento.

ii. L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti.

iii. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di 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 previsto al punto 4.2.2.

iv. L'attività di controllo deve essere adeguatamente documentata e il relativo esito deve essere comunicato ai soggetti indicati al punto 4.3.2.

Soluzione DB.

L'attività di controllo degli alert è demandata, per il Gruppo DB S.p.A, alla U.O. Operational Risk Management (ORM).

ORM è l'unità preposta a ricevere le segnalazioni dell'applicativo Privacy PG2 e ad effettuare, esclusivamente su queste segnalazioni, le verifiche di volta in volta necessarie.

Ove siano ravvisati elementi dai quali sia possibile desumere un comportamento anomalo, l'ORM eseguirà una specifica analisi utilizzando anche l'"interfaccia Client", dandone comunicazione immediata al dipendente interessato, con indicazione della verifica in corso e coinvolgendo ove necessario:

- Il gestore della relazione
- La struttura Human Resources
- La struttura Compliance
- Il responsabile del trattamento dei dati

al fine di verificare l'esistenza di eventuali profili di "trattamento illecito" di dati bancari.

Al termine dell'analisi, qualora dovessero emergere connessi profili di particolare gravità, verrà inviata una comunicazione al dipendente interessato.

Qualora l'ORM ravvisasse un "trattamento illecito", la U.O. Compliance procederà, come richiesto dal Provvedimento del Garante, a segnalare al cliente interessato e al Garante le operazioni di

trattamento illecito effettuate sui dati personali allo stesso riferiti, senza fornire alcuna indicazione in ordine ai dati del dipendente cui risulti imputabile l'eventuale trattamento illecito.

3.1 Definizioni

Description *(fonte Linea Guida ABI Lab)*	
Dati Bancari	Secondo quanto riportato dall'Autorità nel Provvedimento del luglio 2013, per Dati Bancari si intendono le informazioni concernenti la **situazione economica e patrimoniale del cliente,** gestiti nell'ambito della conduzione delle operazioni bancarie di natura dispositiva e/o di consultazione. In tal senso, costituiscono esempi tipici di dati bancari quelli contenuti negli estratti conto, quelli relativi alle operazioni attive o passive portate a termine sui conti correnti e, in generale, le movimentazioni conseguenti ad attività connesse al rapporto contrattuale in essere con i Clienti.
Operazioni Dispositive	Per **Operazioni Dispositive** si intendono l'insieme di **operazioni** che comportano una **movimentazione economica e/o una variazione patrimoniale**, immediata o differita, per conto dei clienti o per conto proprio (e.g. versamento, prelievo, bonifico, operazioni su titoli, etc.).
Operazioni di Interrogazione	Per **Operazioni di Consultazione (Inquiry)** si intendono quelle **operazioni** che comportano la possibilità di **visualizzare dati della clientela** in essere o potenziale, gestiti per **lo svolgimento** di attività bancarie (e.g. visualizzazione saldo di conto corrente, visualizzazione movimenti di conto, etc.).
Utenti incaricati del trattamento	Si tratta degli Utenti abilitati all'utilizzo delle applicazioni
Persone Fisiche	Sono da intendersi come Persone Fisiche quelle definite tali nell'anagrafica aziendale (nota tecnica. SAE 600 o 700 e tipo nominativo di tipo 1 o 3)
U.O. ORM	Unità Organzzativa Operational Risk Management della Deutsche Bank S.p.A.. Unità operativa di secondo livello indipendente dalla struttura a cui è affidato il trattamento dei dati bancari dei clienti.
GROUP AUDIT	Funzione di controllo di terzo livello che effettua le verifiche in modo indipendente su tutti i processi aziendali.
Accessi anomali, comportamenti anomali o a rischio, legittimità e liceità degli accessi, trattamento illecito	Terminologia utilizzata nel Provvedimento. Da intendersi come ad esso riferita.

3.2 *Lista delle Applicazioni*

cr_online-IT	TP SPORTELLO BACK-END-IT
FIDI-2000-IT	DB-SAS-IT
Sportello Web-Back End IT	DDWAY SEPA DD
db-Entry Security Order-IT	Host Interfaces-IT
FF HORIZON-FA Portal	Ramses+-IT
WebApps	GEPA-IT
DB Action-IT	PAPEN-IT
EasyCred-DBM	C3Register-DBSPA_FF
EasyCred-EasyCred Sofia	Compliance Qlikview MIS-Compliance
WeFid-IT	PAPEN WEB
Capital Gain-IT	DB-FUTURES-FE-IT
Centrale allarme Interb.-IT	ASSEGNI DI C/C-IT
NEW AML-F&Futuro	DB-CURRENCY OPTIONS-IT
NEW AML-DB Spa	INCACREDIT-IT
BANCA COLLOCATRICE-IT	IASCREDIT-IT
Smart-Regulatory Reporting-DBM	Foreign Application-IT
UFFICIO CR-CRA	ASS.CIRCOLARI/BONIFICO-IT
Ala	ParagonSME-Italy
Prestitempo DWH-IT Business Reporting	MVS Trader IT
db-DWH Deutsche Credit Card-Reporting	SAP Repository-IT
MA Reports-IT	M.I.S.-IT
CSI-Italy	SAP Banking-International
Gestioni Patrimoniali	SAP Bank Analyzer-International
MPP	Outsourcing of the administrative data loading
NEW SCALARE DS FINANCE-IT	GIANOS 3D-IT
SYGES-IT	Judicial Research-1
DOMESTIC BULK PAYMENTS-IT	Smart-Regulatory Reporting-Bankit
BONIFICI-IT	B2PRO Audit Trail-IT
ORDINI PERMANENTI-IT	FUGWEB-IT

MUTUI-ARTIGIANCASSA-IT	PORTAFOGLIO EFFETTI GESIN WEB
db-Smart-ISS-IT	Nuovo Credito al Consumo
MAPS	E-BAAS BANCASSICURAZIONE-IT
New Insurance Platform (Sostituzione di E-BAAS)	Front End Prestitempo-IT
Microdata Optical Service	CHECK TRUNCATION-IT
BRAIN2K FRONT END-IT (KCCS)	ESITO ELETTRONICO-IT
SFE - Sales Front-End-Activa 1.0-IT	STANZA ASSEGNI-IT