Verbale di accordo

In Spoleto, in data 14 maggio 2014

tra

- Casse di Risparmio dell'Umbria S.p.A.

e

- gli Organismi Sindacali Aziendali FABI, FIBA/CISL, FISAC/CGIL, UILCA di Casse di Risparmio dell'Umbria S.p.A.

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;

- 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;

- 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;

- il Protocollo delle Relazioni Industriali di Gruppo 24 febbraio 2014 assegna:
  - alla Delegazione Sindacale di Gruppo tutte le competenze demandate dalla normativa di legge e di settore al secondo livello di contrattazione. Per i casi in cui la legge individua espressamente il solo livello aziendale la Delegazione definisce accordi quadro da recepire presso le Società;
  - al Comitato di Consultazione la preventiva valutazione degli eventuali interventi che si rendano di volta in volta necessari al fine di assicurare che le scelte adottate circa gli impianti, le apparecchiature e le modalità operative rispondano ai principi condivisi con l'Accordo Quadro 1° febbraio 2011 sull'applicazione del ridetto art. 4 L. n. 300/1970;

- in applicazione di quanto precede, in data 12 maggio 2014 Intesa Sanpaolo in qualità di Capogruppo e le Delegazioni Sindacali di Gruppo hanno sottoscritto l'accordo quadro, che qui si dà integralmente trascritto, che definisce i principi e linee guida valevoli per tutte le società del gruppo rientranti nell'ambito di applicazione del Provvedimento del Garante per la protezione dei dati personali del 12 maggio 2011, n. 192;

si conviene quanto segue:

- la premessa forma parte integrante e sostanziale del presente Accordo che:
  - si applica a tutte le unità produttive di Casse di Risparmio dell'Umbria;
  - conferma che le soluzioni informatiche presentate sono idonee al 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* 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 di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata,

  unitamente agli ulteriori dati contenuti nell'allegato 1.

  Nel caso in cui si evidenziasse la necessità di tracciare ulteriori dati rispetto a quelli qui elencati e contenuti nell'allegato 1, le integrazioni saranno oggetto di informativa – ai sensi e per gli effetti del Protocollo Relazioni Industriali 24 febbraio 2014 – a livello di Comitato di Consultazione e, successivamente, a livello aziendale.

- 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.

- Le specifiche tecniche, riportate nell'allegato 1, formano parte integrante del presente accordo. Le eventuali future modifiche saranno sottoposte, come detto, al Comitato di Consultazione e costituiranno anch'esse parte integrante del presente accordo; successivamente saranno oggetto di illustrazione in sede aziendale e conseguentemente costituiranno parte integrante anche degli accordi aziendali.

- 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.

- 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 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 sarà 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, potranno essere previste, ove necessario, specifiche attività formative retribuite.

- In sede aziendale saranno effettuati, a richiesta, incontri di verifica annuale in merito all'applicazione degli accordi in materia con riferimento al numero di *alert* generati.

- Il Comitato di Consultazione è informato in ordine alla/e unità organizzativa/e cui è tempo per tempo affidato il trattamento dei dati bancari dei clienti in base a quanto previsto dal Provvedimento di cui trattasi, nonché sulle modalità di indagine a campione.

- Per quanto altro non espressamente richiamato nel presente Accordo, si fa rinvio alle prescrizioni del Provvedimento del Garante per la protezione dei dati personali della clientela.

Casse di Risparmio dell'Umbria S.p.A.

FABI

FIBA/CISL

FISAC/CGIL

UILCA

Tracciatura delle operazioni Bancarie

SCHEDA ESPLICATIVA
Dettagli tecnici base dati

Allegato n. 1 - Appendice all'Accordo (parte 1 di 2)

Caratteristiche tecniche	Base dati dipartimentale, ambiente dedicato collocato in infrastruttura standard. Prodotto DB standard di mercato. Previsto salvataggio di backup giornaliero secondo processi standard.
ubicazione	Server farm Moncalieri
Termine di conservazione	24 mesi
Modalità accesso	Con riconoscimento ruoli e profili sistemistici secondo processi standard.

Dettagli tecnici *log* e flussi

Caratteristiche tecniche	Flussi di dati dipartimentali e host, generati e gestiti su infrastruttura standard Moncalieri, Spediti e ricevuti mediante i processi e gli strumenti di trasferimento file standard.
ubicazione	Server farm Moncalieri e Host Moncalieri.
Termine di conservazione	24 mesi a destinazione
Modalità accesso	Con riconoscimento ruoli e profili sistemistici secondo processi standard

Tracciatura delle operazioni Bancarie

SCHEDA ESPLICATIVA

Descrizione del processo e caratteristiche tecniche delle elaborazioni

Allegato n. 1 - Appendice all'Accordo **(parte 2 di 2)**

Ai fini della tracciatura delle operazioni bancarie come richiesto dal provvedimento emesso 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 informatiche nelle basi dati, tutte in infrastruttura standard presso il sito di Moncalieri. Le informazioni registrate sono esclusivamente le informazioni richieste dal provvedimento, ossia:
    a. il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso (user di chi ha eseguito l'operazione);
    b. la data e l'ora di esecuzione;
    c. il codice della postazione di lavoro utilizzata;
    d. il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato (codice fiscale);
    e. la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata - es. numero del conto corrente, fido/mutuo, deposito titoli -, (identificativo del rapporto oggetto, filiale del rapporto, forma tecnica del rapporto);

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 presso il sito di Moncalieri. Le strutture tecnologiche utilizzate sono standard e di mercato.

Le ulteriori informazioni memorizzate sono le seguenti:

f. codice della banca/società in cui è eseguita l'operazione;
g. identificativo dell'applicazione utilizzata;
h. cognome e nome di chi ha eseguito l'operazione;
i. ente di appartenenza del soggetto che ha eseguito l'operazione.

Nel caso in cui chi ha eseguito l'operazione sia un utente esterno:

j. user del riferimento interno;
k. cognome e nome del riferimento interno;
l. ente di riferimento interno.

Nel caso in cui l'operazione sia indirizzata ad un identificativo di cliente o rapporto specifico:

m. super NDG/NSG del cliente oggetto dell'operazione;
n. anagrafica del cliente oggetto dell'operazione;
o. filiale di portafoglio;
p. codice portafoglio;
q. matricola gestore;
r. cognome e nome gestore;

Nel caso in cui l'operazione non sia indirizzata ad un identificativo di cliente o rapporto specifico (ricerche massive):

s. parametri di ricerca inseriti: l'insieme dei parametri inseriti che consentono di individuare il contenuto dei dati richiesti in estrazione;

5. reporting: sulla base dati è prevista la creazione di report con interfaccia standard di Business Intelligence. Accesso consentito ai referenti dell'unità di riferimento Privacy competente per società secondo i ruoli ed i processi di autenticazione standard. Gli accessi sono, a loro volta, tracciati secondo le modalità e le regole definite dal Provvedimento.