ACCORDO EX ART. 4, COMMA 2, L.N. 300/1970 SULL'APPLICAZIONE DEL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 12 MAGGIO 2011, N. 192

Il giorno 17/09/2014, a Parma

tra

le seguenti Aziende, d'ora in poi denominate tutte insieme "Gruppo":

Cassa di Risparmio di Parma e Piacenza S.p.A. (Cariparma), anche in qualità di Capogruppo del Gruppo Cariparma Crédit Agricole,

Banca Popolare FriulAdria S.p.A. (FriulAdria),

Cassa di Risparmio della Spezia S.p.A. (Carispezia),

Crédit Agricole Leasing Italia S.r.l. (CALIT)

e

le sottoscritte Delegazioni Sindacali di Gruppo delle OO.SS.:

DIRCREDITO FD

FABI

FIBA/CISL

FISAC/CGIL

SINFUB

UGL Credito

UILCA

d'ora in poi denominate complessivamente "OO.SS."

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" (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, in seguito ulteriormente prorogato con il Provvedimento n. 257 del 22 Maggio 2014;
4. Il provvedimento 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, comma1, 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;

Dircredito – Fabi – Fiba/ Cisl – Fisac/ Cgil – Sinfub – Ugl Credito – Uilca

5. Il Provvedimento riguarda le operazioni relative ai clienti -persone fisiche o ditte individuali- degli istituti bancari, di cui al punto che precede, "sia quelle che comportano movimentazione di denaro, sia quella di sola consultazione, c.d. inquiry";

6. 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".

7. 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 su 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".

8. 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".

9. 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".

10. L'art.4 co.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.

11. L'art.114 d.lgs.30 giugno 2003, n.196 stabilisce che "Resta fermo quanto disposto dall'Art.4 della Legge 20 Maggio 1970 n.300".

12. 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".

13. Il Provvedimento definisce "un quadro unitario di misure necessarie e opportune" per tutte le Banche ed i gruppi bancari di cui al punto 4 che precede.

14. 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".

15. 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, le Parti hanno inteso promuovere il raggiungimento delle correlate intese aziendali, tramite uno specifico Accordo quadro nazionale, finalizzato esclusivamente alle esigenze di adempiere al Provvedimento.

16. In data 15 Aprile 2014 è stato quindi sottoscritto, tra ABI e le Organizzazioni Sindacali Nazionali 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 per la stipulazione di intese ex art.4, comma 2, L. n.300/70 in specifica attuazione del Provvedimento in oggetto.

Dircredito – Fabi – Fiba/ Cisl – Fisac/ Cgil – Sinfub – Ugl Credito – Uilca

17. Tale accordo quadro stabilisce 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 del Garante.

18. Tenuto anche conto che il Protocollo delle Relazioni Sindacali del Gruppo Cariparma Crédit Agricole sottoscritto il 19 gennaio 2012 assegna alla Delegazione sindacale di Gruppo la funzione di stipulare intese vincolanti per tutte le Società del Gruppo e le rispettive OO.SS. anche riguardo linee guida e principi di applicazione degli impianti ed apparecchiature di controllo (art.4 L.300/70-impianti audiovisivi) le Parti hanno dato corso ad un ampio confronto a livello di Gruppo finalizzato a verificare la coerenza delle proposte dell'impresa con le vigenti disposizioni in materia ed il predetto Accordo quadro ed, inoltre, a stipulare i conseguenti accordi ex art. 4, comma 2, L. n. 300 del 1970.

19. Nell'ambito di detto confronto, le Parti hanno condiviso di sottoscrivere l'accordo ai sensi dell'art. 4 L. 300/70 con le Delegazioni di Gruppo, valevole per tutte le società del Gruppo rientranti nell'ambito di applicazione del Provvedimento.

20. Il Gruppo ha illustrato alle Delegazioni Sindacali di Gruppo, nel corso di appositi incontri, le caratteristiche ed il funzionamento degli strumenti informatici predisposti al fine di adeguare i propri sistemi alle prescrizioni del Provvedimento,

si conviene quanto segue

1. La premessa costituisce parte integrante e sostanziale del presente Accordo, che si applica a tutte le unità produttive delle Banche e Società facenti parte del Gruppo Cariparma Crédit Agricole e a tutti i lavoratori incaricati dall'Azienda dei trattamenti riconducibili all'ambito di applicazione del Provvedimento n.192, quali che siano la qualifica, le competenze, l'ambito di operatività e le finalità dei trattamenti che sono tenuti a svolgere. Calit adotterà una soluzione analoga a quella di seguito descritta per principi e garanzie, ma con modalità differenti, in quanto utilizza un sistema informatico diverso e separato rispetto a quello delle Banche; tali modalità sono dettagliate negli specifici allegati tecnici e organizzativi. Si precisa che i dipendenti di Calit non possono accedere ai sistemi di Cariparma e trattano unicamente dati relativi alle operazioni di leasing.

Principi e Sistema di tracciamento

2. Il Gruppo adotta "idonee soluzioni informatiche" per il controllo dei trattamenti condotti sui singoli elementi di informazione, tramite applicazione interattiva, dei dati 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.

3. I sistemi informativi interessati sono impostati ai fini della registrazione dettagliata - anche attraverso un "registratore grafico" delle videate applicative - in 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 inquiry sui dati bancari effettuata da un incaricato, le seguenti informazioni: il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso; il codice Istituto/Banca a cui appartiene il 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 (NDG) ai dati bancari da parte dell'incaricato; il codice applicazione utilizzata per accedere ai dati delle singole tipologie di rapporto contrattuale del cliente.

L'utilizzo del "registratore grafico" consente di tracciare accessi, comandi ed attività eseguite dagli incaricati sui dati della clientela, in appositi fotogrammi (vengono riprodotte le variazioni avvenute sullo schermo sia in fase di input che in quella di output).

Gli ulteriori dati che si rendesse necessario tracciare in quanto funzionali alla realizzazione delle finalità previste dal Provvedimento saranno oggetto di informativa ai medesimi soggetti sindacali firmatari della presente intesa, nel corso di apposito incontro.

4. Il sistema di registrazione dei log garantisce la riservatezza e l'inalterabilità delle informazioni tracciate. Ciò posto, l'accesso al sistema è consentito solo a personale autorizzato e abilitato.

5. I log di tracciamento e le immagini delle operazioni di *inquiry* sono conservati per un periodo di 24 mesi dalla data di registrazione dell'operazione, fatte salve le esigenze di forza maggiore (ad es: richieste delle autorità giudiziarie). Oltre tale limite temporale la conservazione è ammessa in presenza di specifici vincoli di legge.

   Le specifiche tecniche e organizzative apprestate, riportate nei rispettivi allegati, e le eventuali modifiche formano parte integrante del presente accordo, e sono oggetto di un incontro sindacale di illustrazione a livello di gruppo, che verrà ripetuto in caso di significative variazioni.

Sistema di alert

6. 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 relative caratteristiche sono specificate nell'allegato organizzativo del presente accordo.

Controlli

7. Ai sensi del Provvedimento citato 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 normative vigenti.

   b) 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.

   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.

   Le relative specifiche sono dettagliate nell'allegato organizzativo del presente accordo.

Informativa al personale

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 deve essere portata a conoscenza di tutti i lavoratori attraverso specifici e opportuni strumenti (entro la data del 30 settembre 2014 verrà emanata apposita circolare, che sarà altresì pubblicata nella bacheca Privacy presente nelle intranet aziendali del Gruppo). Inoltre, nell'ambito di quanto previsto dall'art. 72 del CCNL del 19 gennaio 2012, potranno svolgersi, ove necessario, specifiche attività formative retribuite.

Incontri di verifica

9. In sede di gruppo saranno possibili, d'intesa tra le Parti, incontri di verifica annuale in merito all'applicazione del presente accordo. In tali occasioni il Gruppo fornirà le statistiche relative al numero e alle tipologie di "alert" con l'indicazione dei c.d. "falsi positivi".

   In ragione delle caratteristiche sperimentali delle attività descritte nell'allegato organizzativo, è previsto un primo incontro di verifica indicativamente nel mese di settembre 2015.

Dircredito – Fabi – Fiba/ Cisl – Fisac/ Cgil – Sinfub – Ugl Credito – Unica

In sede 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.

Disposizioni finali

L'utilizzo degli strumenti regolati dal presente accordo è finalizzato esclusivamente ad adempiere alle necessità illustrate in premessa, con particolare riferimento agli adempimenti previsti dal Provvedimento di cui si tratta. Viene pertanto esplicitamente esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dei dipendenti. L'accesso ai dati inerenti le attività di cui sopra è riservato al personale autorizzato, incaricato ed appartenente alle Funzioni citate nell'allegato organizzativo.

Le implementazioni poste in essere dal Gruppo sono conformi a quanto previsto dall'art. 4 dello "Statuto dei Lavoratori".

Per quanto altro non espressamente richiamato dalla presente intesa si fa rinvio alle prescrizioni del Provvedimento del Garante per la protezione dei dati personali in oggetto e all'Accordo quadro nazionale del 15 aprile 2014.

Letto, confermato e sottoscritto

Le Aziende

Cassa di Risparmio di Parma e Piacenza S.p.A. (anche in qualità di Capogruppo)

Banca Popolare FriulAdria S.p.A.

Cassa di Risparmio della Spezia S.p.A.

Crédit Agricole Leasing Italia S.r.l.

Organizzazioni Sindacali

Dircredito – Fabi – Fiba/ Cisl – Fisac/ Cgil - Sinfub – Ugl Credito - Uilca

Dircredito – Fabi – Fiba/ Cisl – Fisac/ Cgil - Sinfub – Ugl Credito - Uilca

Allegato Tecnico Banche:

Caratteristiche tecniche	Registratore grafico in ambiente dipartimentale Database standard di mercato con dati cifrati Cifratura dati su piattaforma consultazione log Supporto storage con cifratura nativa dati Utilizzo firma e marche temporali su dati raccolti
Ubicazione	Data center Cariparma
Informazioni di base gestite	Accessi singoli: • Codice istituto • Codice NDG cliente interessato • Codice filiale Rapporto cliente interessato • Codice Rapporto cliente interessato • Codice identificativo operatore • Data e ora esecuzione • Codice postazione di lavoro utilizzata • Codice applicazione utilizzata Accessi massivi: • Codice istituto • Codice identificativo operatore • Data e ora esecuzione • Codice postazione di lavoro utilizzata • Codice applicazione utilizzata • Risultato della richiesta
Modalità di accesso	Riconoscimento utenti secondo ruoli e profili. Tracciatura accessi.
Sicurezza fisica	Procedure di backup come da standard di sitema
Termini di conservazione	24 Mesi (salvo esigenze di forza maggiore)
Aggiornamento	Giornaliero
Modalità di alimentazione	• Acquisizione immagini applicative • Acquisizione log applicativi • Normalizzazione dati e generazione log Privacy

Principi e Sistema di tracciamento	L'adempimento degli obblighi normativi è stato attuato con l'implementazione di una struttura informatica che provvede alla registrazione dei log attraverso il sistema, che opera il "collezionamento" e la storicizzazione dei log, separatamente dai sistemi alimentanti. In attuazione di quanto previsto dalle "Disposizioni di vigilanza per le banche in materia di conformità alle norme (*compliance*)", adottate dalla Banca d'Italia il 10/07/2007, per quanto afferisce le operazioni bancarie "dispositive", esse vengono tracciate nel rispetto delle vigenti disposizioni di legge e del principio di riservatezza assicurato tramite il riconoscimento di ruoli e profili del personale autorizzato all'accesso dei dati. Per quanto concerne le operazioni bancarie di inquiry, eseguite dagli incaricati del trattamento, il sistema attiva un meccanismo di monitoraggio, che rileva dati e fornisce indicatori di rischio (c.d. alert). Tali alert sono interpretati ad opera di operatori qualificati, che hanno il compito di rilevare eventuali pratiche comportamentali potenzialmente anomale ossia accessi ai dati bancari di clienti che potrebbero, in tesi, costituire trattamenti illeciti di dati personali. L'attività di raccolta e generazione log ha frequenza giornaliera. Il sistema che raccoglie e gestisce l'insieme dei log e fotogrammi prodotti nel corso della tracciatura è installato in ambiente dipartimentale dedicato, con una base dati protetta da crittografia. I log sono firmati digitalmente con marca temporale dalla Banca. L'accesso alle elaborazioni dei log tramite interfaccia applicativa sarà governata da ruoli e profili organizzativi. Per le strutture operative IT i dati saranno opportunamente mascherati; solo e soltanto le strutture preposte avranno completa visibilità in chiaro delle informazioni raccolte nei log (le strutture sono indicate in "organizzazione attività"). Gli accessi alla piattaforma di gestione Alert sono a loro volta tracciati secondo le modalità e regole definite dal Provvedimento del Garante.
Sistema di alert	Al fine di adempiere agli obblighi normativi, il Gruppo attiva un sistema di "*alerting*" finalizzato a individuare "comportamenti anomali o a rischio" rilevati dallo stesso sistema. Gli alert tengono in considerazione i seguenti elementi: • quantità delle inquiry effettuate (ad esempio, inquiry ripetute con frequenza significativamente diversa rispetto alla normale operatività, a parità di ruolo/profilo, su un determinato cliente o sulla stessa tipologia di rapporti intestati a diversi clienti); • circostanze temporali delle inquiry effettuate (ad esempio, inquiry effettuate fuori dal normale orario di lavoro o in giorni festivi o nei giorni di assenza; frequenza di inquiry significativamente diversa rispetto alla normale operatività in un determinato arco temporale) • unità organizzativa di appartenenza dell'incaricato al trattamento; • struttura di riferimento del cliente (ad esempio la filiale o la Direzione Territoriale) • tipologia dell'operazione (ad esempio, "STCC"); • tipologia di rapporto (ad esempio, conto corrente "vip" o di "over 75", ecc..); • accessi contemporanei da diverse postazioni di lavoro.
Controlli	L'attività di controllo sarà demandata ad una unità organizzativa, o comunque a personale diverso rispetto a quello a cui è affidato il trattamento dei dati bancari dei clienti; tale attività di controllo è, allo stato, demandata alla funzione aziendale competente in materia di Compliance. Tale funzione è competente anche per le verifiche a posteriori, a campione, o a seguito di allarme derivante da sistemi di *alerting* e di *anomaly detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati. Inoltre, il Servizio Sicurezza Logica effettua i predetti controlli sull'integrità dei dati e delle procedure informatiche adoperate per il trattamento; nonché per le verifiche periodiche sulla corretta conservazione dei file di *log* per il periodo sopra previsto. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate (per quanto

	concerne l'ambito del Servizio Sicurezza Logica), alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate (per quanto concerne l'ambito dei "Referenti Privacy" e del R.I.N. Privacy").
Organizzazione delle attività	Stante la necessità di declinare - per ciascuna tipologia di dati bancari ed operazioni bancarie identificate - quali siano i comportamenti che potrebbero configurarsi come anomali e, conseguentemente, originare messaggi di alert, l'organizzazione delle attività necessarie ad adempiere agli obblighi normativi sarà oggetto di una adeguata fase sperimentale, della durata di circa un anno. La registrazione dei log e la generazione tecnica degli *alert* è demandata al Servizio Sicurezza Logica, che effettua una elaborazione specifica e distinta per ciascuna Banca del Gruppo. Sulla base dei dati e delle segnalazioni provenienti dal Servizio Sicurezza Logica gli alert vengono fatti oggetto di interpretazione ad opera dei "Referenti Privacy" (per dati / segnalazioni relativi a FriulAdria e Carispezia) e del "R.I.N. Privacy" (per dati / segnalazioni relativi a Cariparma), quali funzioni incaricate a gestire la fase sperimentale. Tali strutture assolvono il compito di rilevare eventuali pratiche comportamentali potenzialmente anomale ossia accessi ai dati bancari di clienti che possono costituire trattamenti illeciti di dati personali. Dei casi non archiviati in quanto ritenuti potenzialmente anomali verrà data apposita e tempestiva comunicazione agli interessati che potranno prendere visione della relativa documentazione. Qualora dovessero emergere elementi dai quali si possano desumere le predette pratiche, i "Referenti Privacy" o il "R.I.N. Privacy" provvedono a segnalare l'evento alla Direzione Governo Risorse Umane, per l'effettuazione degli approfondimenti necessari e la gestione delle eventuali responsabilità.

Dircredito – Fabi – Fiba/ Cisl – Fisac/ Cgil – Sinfub – Ugl Credito – Uilca

Allegato Tecnico CALIT:

Caratteristiche tecniche	Database di LOG delle disposizioni e delle inquiry eseguite sui dati della clientela a seguito di un uso interattivo del Sistema Informativo di CALIT (NSIL) Database dedicato per la storicizzazione del DB di LOG
Ubicazione	Data center Pont Saint Martin
Informazioni di base gestite	accessi che producono informazioni a livello di dettaglio dei dati della clientela • Codice NDG cliente interessato • Codice Rapporto cliente interessato • Codice identificativo operatore • Data e ora di esecuzione • Codice postazione di lavoro utilizzata • Codice applicazione utilizzata
Modalità di accesso	Riconoscimento utenti secondo ruoli e profili. Tracciatura accessi.
Sicurezza fisica	Procedure di backup come da standard di sistema
Termini di conservazione	24 Mesi (salvo esigenze di forza maggiore)
Aggiornamento	Giornaliero
Modalità di alimentazione	• Acquisizione log applicativi

Allegato Organizzativo CALIT

Principi e Sistema di tracciamento	L'adempimento degli obblighi normativi è stato attuato con idonee soluzioni informatiche per il controllo dei trattamenti condotti sui singoli elementi d'informazione presenti sulle applicazioni, ai sensi di quanto prescritto dal Garante Privacy con il Provvedimento. Il Database di LOG tiene traccia di tutte le attività interattive essendo innestato nelle funzioni base del Sistema Informativo NSIL.
Sistema di alert	Al fine di adempiere agli obblighi normativi, è stato attivato un sistema di "*alerting*" finalizzato a individuare "comportamenti anomali o a rischio" rilevati dallo stesso sistema. Gli alert tengono in considerazione i seguenti elementi: • quantità delle inquiry effettuate (ad esempio, inquiry ripetute con frequenza significativamente diversa rispetto alla normale operatività, a parità di ruolo/profilo, su un determinato cliente o sulla stessa tipologia di rapporti intestati a diversi clienti); • circostanze temporali delle inquiry effettuate (ad esempio, inquiry effettuate fuori dal normale orario di lavoro o in giorni festivi o nei giorni di assenza; frequenza di inquiry significativamente diversa rispetto alla normale operatività in un determinato arco temporale) • unità organizzativa di appartenenza dell'incaricato al trattamento; • tipologia di rapporto • accessi contemporanei da diverse postazioni di lavoro.
Controlli	L'attività di controllo sarà demandata ad una unità organizzativa, o comunque a personale diverso rispetto a quello a cui è affidato il trattamento dei dati dei clienti, in accordo con la funzione aziendale competente in materia di Compliance. Il sistema dei controlli comprende anche verifiche a posteriori, a campione, a seguito di allarme, sulla legittimità e liceità degli accessi ai dati effettuati dagli Incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento, sulla corretta conservazione dei file di LOG. L'attività di controllo segue i processi aziendali e la normativa interna già in essere ed è svolta dalle competenti Funzioni di Controllo. In tal senso, anche tale tipologia di controlli è documentata e rende possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.
Organizzazione delle attività	Stante la necessità di declinare quali siano i comportamenti che potrebbero configurarsi come anomali e, conseguentemente, originare messaggi di alert, l'organizzazione delle attività necessarie ad adempiere agli obblighi normativi sarà oggetto di una adeguata fase sperimentale, della durata di circa un anno. La registrazione dei log e la generazione tecnica degli *alert* è demandata al Servizio Personale Organizzazione e Sistemi Informativi di CALIT. Sulla base dei dati e delle segnalazioni provenienti dal Servizio Personale Organizzazione e Sistemi Informativi gli alert vengono fatti oggetto di interpretazione ad opera dei "Referenti Privacy" di CALIT quali funzioni incaricate a gestire la fase sperimentale. Tali strutture assolvono il compito di rilevare eventuali pratiche comportamentali potenzialmente anomale ossia accessi ai dati dei clienti che possono costituire trattamenti illeciti di dati personali. Dei casi non archiviati in quanto ritenuti potenzialmente anomali verrà data apposita e tempestiva comunicazione agli interessati che potranno prendere visione della relativa documentazione. Qualora dovessero emergere elementi dai quali si possano desumere le predette pratiche, i "Referenti Privacy" provvedono a segnalare l'evento al Servizio Personale Organizzazione e Sistemi Informativi che si attiverà per l'effettuazione degli approfondimenti necessari e la gestione delle eventuali responsabilità.

Dircredito - Fabi - Fiba/ Cisl - Fisac/ Cgil - Sinfub - Ugl Credito - Uilca