Accordo di attuazione dell'Accordo Quadro nazionale di settore sul Provvedimento n. 192 12 maggio 2011 del Garante per la protezione dei dati personali

Allegato n. 2

Struttura del Modello

1. Il Gruppo UniCredit, ai sensi del Provvedimento n. 192/2011, adotta un modello organizzativo e relativi processi e connesse soluzioni informatiche, secondo quanto illustrato e disciplinato nel presente Accordo.
2. Il modello, i processi ed il Sistema Informativo vengono adottati in modo uniforme in tutte le aziende del Gruppo soggette alle disposizioni del Provvedimento del Garante.
3. L'attuazione delle disposizioni del Provvedimento è realizzata mediante l'utilizzo di prodotti informatici ***SIEM*** (Security Information and Event Management) e di ***BUSINESS INTELLIGENCE*** volti alla conservazione delle informazioni riferite alle operazioni bancarie ed all'attivazione di *alert* diretti all'individuazione di comportamenti potenzialmente anomali o a rischio relativi alle operazioni di interrogazione eseguite dai dipendenti incaricati del trattamento.
4. Attraverso l'adozione di tali sistemi, viene garantita la riservatezza e l'inalterabilità dei log e delle informazioni.

Sistema di tracciamento degli accessi ai sistemi e di conservazione dei relativi file di Log

1. Al fine di ottemperare esclusivamente a quanto richiesto dal Provvedimento in tema di tracciamento delle operazioni bancarie –sia di tipo dispositivo, sia di semplice visualizzazione- effettuate utilizzando informazioni concernenti la situazione economica e patrimoniale del cliente e quando consistono o derivano dall'uso interattivo dei sistemi, viene garantita la "registrazione dettagliata, in un apposito log" delle operazioni effettuate da tutti gli "incaricati" del trattamento.
2. Il Gruppo UniCredit ha adottato sistemi SIEM (Security Information and Event Management) volti alla conservazione sicura dei log ed al fine di garantirne l'integrità e l'immodificabilità.
3. In particolare, il "sistema" prevede la raccolta e l'archiviazione, in modo automatico, delle informazioni corrispondenti al "contenuto minimo" previsto dall'Autorità Garante, 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.

4. Il Gruppo UniCredit ha inoltre provveduto alla memorizzazione anche delle seguenti informazioni:

   - ✓ Codice dell'applicazione utilizzata per effettuare l'accesso ai dati bancari;
   - ✓ Struttura di appartenenza dell'incaricato.

5. I Sistemi conservano per un periodo di **24 mesi** decorrenti dalla data di esecuzione dell'operazione, salvo esigenze di forza maggiore, i file di log garantendone le caratteristiche di integrità e immodificabilità ed

assicurando le idonee misure di sicurezza stabilite dal D. Lgs. 196/2003. La conservazione oltre tale limite temporale è ammessa solo in presenza di specifici vincoli di legge in materia.

Sistema di Alert

1. Il Gruppo UniCredit ha attivato, attraverso idonei strumenti di Business Intelligence, *"specifi alert"* finalizzati ad individuare "*comportamenti anomali o a rischio*" sulla base di specifiche regole di alert, ossia:

   - ✓ Interrogazioni effettuate fuori dalla fascia oraria operativa della struttura (regola applicata alle strutture centrali e di rete);
   - ✓ Frequenza di interrogazioni in relazione all'indice di movimentazione del rapporto (regola applicata a strutture centrali e di rete);
   - ✓ Interrogazioni su rapporti/prodotti con saldo superiore ad un certo valore definito (regola applicata a strutture di rete);
   - ✓ Interrogazioni su rapporti non radicati/gestiti rispettivamente presso o dalla struttura organizzativa di appartenenza del dipendente (regola applicata alle strutture di rete).

2. I principi delle regole di alert sono stati definiti dalla Capogruppo e sono stati adattati alle specifiche realtà delle diverse Società del Gruppo.

3. Al fine della rilevazione di comportamenti potenzialmente anomali, confluiscono inoltre nei sistemi di Business Intelligence anche le seguenti ulteriori informazioni di arricchimento:

   - ✓ dati relativi al dipendente che ha effettuato l'interrogazione, ivi compresi informazioni inerenti alla sua struttura di appartenenza: matricola, ruolo, orario di lavoro della Struttura, codice e Comune ove è ubicata la Struttura;
   - ✓ dati relativi al cliente oggetto dell'interrogazione: codice cliente, anagrafica cliente, Comune di residenza, tipo cliente. codice gestore;
   - ✓ dati relativi al rapporto contrattuale del cliente: numero rapporto, tipo rapporto, data ultimo movimento.

4. Il sistema di Business Intelligence effettua, in funzione dei parametri sopra definiti, i controlli sui dati ricevuti, generando una segnalazione di anomalia (*alert*) nel caso in cui vengano superate specifiche soglie stabilite, costituite da un numero predeterminato da ciascuna Società del Gruppo, oltre il quale le *inquiry* sono presunte come anomale.
5. Le evidenze informatiche riferite alla generazione degli alert saranno conservate nei sistemi di business intelligence per il solo tempo necessario ai successivi interventi di controllo e di verifica. A seguito dell'inoltro alla Strutture deputate ai Controlli di primo livello, le stesse verranno cancellate dai suddetti sistemi.

Audit Interno e Monitoraggio degli Alert

1. L'attività di controllo è demandata, ai sensi del Provvedimento del Garante *"a unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti"*.
2. Ai sensi del Provvedimento, "*i controlli devono comprendere anche verifiche a posteriori, a campione o in seguito ad 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".

3. In particolare vengono identificate per tutto il Gruppo le seguenti strutture di Controllo di Primo e di Secondo Livello.

   Al *Primo Livello* intervengono le strutture di internal control. Al *Secondo Livello* intervengono le strutture di compliance ed eventualmente quelle di internal audit;

   Tali strutture sono quelle preposte a ricevere le segnalazioni dei Sistemi di Business Intelligence e ad effettuare le verifiche di volta in volta necessarie.

4. Ai sensi del Provvedimento del Garante "la gestione dei dati bancari deve essere 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".
5. Come previsto dal Provvedimento, "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, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate".
6. Verranno memorizzati anche gli accessi dei vari incaricati delle strutture di Controllo ai Sistemi di Business Intelligence, indispensabili per svolgere le anzidette attività.
7. Le Strutture di Controllo aziendali di secondo livello, in presenza di esito positivo dei controlli effettuati, segnaleranno tale circostanza alle Strutture aziendalmente competenti, per valutare l'eventuale comunicazione al Garante per la Protezione dei dati personali ovvero alla clientela di quanto riscontrato (il Provvedimento definisce queste comunicazioni come misure opportune non come misure necessarie).

Informativa e formazione ai Dipendenti

1. 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.
2. Inoltre, nell'ambito di quanto previsto dall'art. 72 del ccnl 19 gennaio 2012, possono svolgersi, ove necessario, specifiche attività formative retribuite.
3. In particolare, nella fase di prima attuazione del Provvedimento:
   a. viene pubblicata/trasmessa news con informativa sul Provvedimento e sugli strumenti utilizzati;
   b. viene aggiornata l'informativa resa agli incaricati al trattamento dei dati;
   c. viene messo a disposizione di tutto il personale il modulo formativo a fruizione obbligatoria retribuita "Privacy e sicurezza dei dati", contenente una specifica sezione sulle prescrizioni e gli adempimenti del Provvedimento del Garante.