



Tresivio (SO), 22 settembre 2014

Le Delegazioni Sindacali ed i Rappresentanti del Gruppo Credito Valtellinese si sono incontrati il giorno 17/9 per definire il calendario degli incontri riguardante l'Aggiornamento del Piano strategico 2014-2016, nonché alcuni aspetti applicativi dell'accordo 8/7 sul tracciamento delle operazioni bancarie. Sul primo aspetto che interessa tutti, in quanto verterà sulla nuova procedura esuberi e la complessiva riorganizzazione degli sportelli del Gruppo, le parti si incontreranno a partire dal 13 ottobre, data in cui si presume sarà conclusa la "valutazione approfondita" di Bankitalia per conto della BCE (AQR – STRESS TEST).

**Vi invitiamo ora a leggere con attenzione nel vostro interesse quanto segue in materia di privacy sulla tracciabilità dei dati.**

## **Provvedimento n. 192 Garante Privacy**

### **Tracciamento delle operazioni bancarie**

Il Provvedimento del Garante n. 192 del 12/5/2011 ha prescritto, **a partire dal 30/09/2014**, a tutela dei dati personali della clientela, una serie di misure riguardanti la circolazione delle informazioni dei clienti in ambito bancario ed il tracciamento delle operazioni.

Il Provvedimento del Garante ha l'obiettivo di assicurare il controllo delle attività svolte sui dati dei clienti da parte di ciascun dipendente, impartendo a tutte le banche l'adozione di specifiche soluzioni informatiche che consentano l'individuazione delle operazioni effettuate dai dipendenti sui dati dei clienti, anche nel caso di sola consultazione.

Il coinvolgimento sindacale, raccomandato anche dal Garante della Privacy, si è reso necessario per gli evidenti rischi connessi a un "possibile incrocio" tra il diritto alla privacy della clientela e il diritto dei lavoratori a non essere oggetto di controllo a distanza.

Nell'incontro del 17/09 le OO.SS. hanno più volte chiesto chiarimenti sulle modalità applicative dei cosiddetti *alert*. Il Garante ha infatti impartito a tutte le aziende bancarie l'attivazione di particolari programmi informatici atti a svolgere, in maniera automatica attraverso algoritmi prefissati, un'attività di analisi degli accessi da parte dei dipendenti ai dati dei clienti, per individuare possibili comportamenti anomali o a rischio in ordine alla liceità degli accessi effettuati dai dipendenti.

Alle nostre richieste di volere specificare dettagliatamente in quali casi gli alert vengano generati e come questi vengano gestiti dalle competenti funzioni di auditing interni. L'Azienda non ha voluto fornire alcuna precisazione in merito.

Le OO.SS. non possono assolutamente condividere un simile comportamento aziendale, che riteniamo quindi tutt'altro che corretto e limpido verso le colleghi e i colleghi che saranno a breve inconsapevoli destinatari di queste nuove procedure.

L'Azienda si è limitata a ribadire l'assoluta volontà di attenersi alle sole prescrizioni del Garante escludendo, come già previsto dall'accordo dell'8/7, «ogni finalità diretta o indiretta di controllo a distanza dei lavoratori contraria a quanto previsto dalle vigenti disposizioni di legge (art. 4 Legge

300/1970)», ma non ha voluto fornire alcun dettaglio in merito agli alert che, se operati correttamente e con buon senso responsabile, sarebbero a nostro avviso a garanzia dei colleghi stessi, avvertendoli in tempo di eventuali comportamenti non corretti.

Rispetto a tale comportamento aziendale per nulla collaborativo abbiamo intanto sollecitato l'attivazione degli istituti contrattuali previsti dal CCNL vigente, sia prevedendo adeguati momenti formativi, sia mediante riunioni durante l'orario di lavoro, con esclusione dell'orario di sportello. A tale scopo torneremo presto, anche come osservatorio sulla formazione, sulla novità denominata "CREVAL ACADEMY" e sulla sua formula, giocata sull'ambiguità della volontarietà, per incentivare l'esecuzione della formazione professionale al di fuori dall'orario di lavoro.

Da parte nostra svolgeremo tutte le verifiche del caso, anche in campo legale, in quanto se è vero che gli alert entreranno a far parte della normativa interna aziendale, è anche vero che questa deve essere resa chiara e trasparente a tutti i colleghi. L'Azienda ha l'obbligo contrattuale, di informare e formare tutti i colleghi interessati su una normativa così delicata e che rischia di diventare pesantemente invasiva.

Ricordiamo ora brevemente cosa ha previsto l'accordo sindacale, sottoscritto l'8/7, che ha inteso introdurre solamente i requisiti minimi delle previsioni del Garante, riducendo così al minimo i possibili rischi di un "controllo a distanza" a danno dei lavoratori.

- Per ogni operazione, anche di inquiry, che comporti l'accesso ai dati bancari su rapporti intrattenuti **con persone fisiche**, registrazione in un file di log contenente:
  - codice identificativo del lavoratore
  - data/ora di esecuzione
  - codice della postazione di lavoro
  - codice cliente
  - tipologia del rapporto contrattuale oggetto dell'operatività.
- Conservazione dei dati per 24 mesi, salvo la presenza specifica di vincoli di legge in materia.

**La normativa di legge prevede che ognuno risponde personalmente di quanto fatto con la propria matricola**, anche in caso di semplici consultazioni. Raccomandiamo che tutte le operazioni bancarie, consultazioni di dati, stampe di posizioni dei clienti, etc siano sempre ed esclusivamente svolte dai colleghi direttamente interessati nell'ambito del compito svolto. In tutti gli altri casi in cui ove non vi sia nesso diretto fra compito svolto e richiesta ricevuta, potrà esservi richiesta adeguata giustificazione e documentazione. In questi casi richiedete quindi sempre espressa autorizzazione scritta da parte del responsabile se volete dormire sonni tranquilli.

Raccomandiamo inoltre la massima attenzione, per evitare quei comportamenti dettati spesso da prassi operative ormai consolidate ma vietate dalla normativa, come ad es.: informazioni di qualunque genere sui rapporti date telefonicamente; operazioni, d'ora in avanti, anch'esse assoggettate a tracciatura che, al ricorrere di determinate situazioni, possono generare degli alert e configurare, per la loro natura, accesso illecito.

Nell'invitarvi a prestare la massima attenzione, sarà nostro preciso impegno verificare, con il supporto di tutti i colleghi interessati che tali normative, introdotte dal Garante Privacy a tutela dei clienti, siano puntualmente applicate dall'Azienda anche nel rispetto degli interessi e della dignità delle lavoratrici e dei lavoratori del Gruppo Creval.

Vi terremo tempestivamente informati su eventuali modifiche o variazioni in materia rimanendo sempre a vostra disposizione per eventuali approfondimenti.