CGIL FISAC UNICREDIT

BLOC-NOTES

notizie e riflessioni per le iscritte e gli iscritti
Fisac/CGIL di UniCredit Group

www.fisacunicredit.eu fisac cgil unicredit

PRIVACY: Misure per Banche e Poste Italiane relative alla circolazione delle informazioni dei clienti e loro tracciabilità

Riferimenti normativi:

- **Legge 300/70 (Statuto dei Lavoratori)**
- **Provvedimento n° 192/2011 del Garante per la protezione dei dati personali**
- **Jobs Act (D. Lgs n. 151 del 14/09/2015)**
- **Regolamento Generale sulla protezione dei dati UE 2016/679 (GDPR - *General Data Protection Regulation*)**

Il 22 maggio 2014 è stato sottoscritto tra UniCredit e le delegazioni di Gruppo delle Organizzazioni Sindacali, una intesa che dà attuazione all'Accordo Quadro Nazionale di Settore sul **Provvedimento n° 192/2011 del Garante per la protezione dei dati personali**.

Bisogna porre estrema attenzione a questo Provvedimento, in quanto, in caso di violazione del medesimo, le contestazioni disciplinari elevate dall'Azienda sono estremamente probabili.

IL GARANTE HA DISPOSTO CHE TUTTE LE OPERAZIONI DI ACCESSO AI DATI DEI CLIENTI, SIA PER MOVIMENTAZIONE CHE PER SEMPLICE CONSULTAZIONE, DOVRANNO ESSERE TRACCIATE E CHE SIA SEMPRE IDENTIFICABILE L'OPERATORE CHE ESEGUE L'ACCESSO.

Tale disposizione ha determinato, di fatto, la possibilità di un controllo a distanza dei lavoratori e, come tale, **ha richiesto un'apposita regolamentazione per tutelare i dipendenti da ogni possibile abuso ai sensi dell'articolo 4 della L. 300/70 – Statuto dei Lavoratori**.

STRUMENTI DI LAVORO E STRUMENTI DI CONTROLLO

A quanto già detto bisogna aggiungere che il **Jobs Act (D. Lgs n. 151 del 14 settembre del 2015) ha riscritto, tra l'altro, proprio l'art. 4 dello Statuto dei Lavoratori sul controllo a distanza dei lavoratori, fissando un regime diverso a seconda del tipo di strumento utilizzato:**

- **Strumenti che consentono il controllo del lavoratore** (es. videosorveglianza);

- **Strumenti di lavoro** (personal computer, smartphone, ecc.).

La revisione della disciplina dei controlli sui lavoratori ha tenuto conto dell'evoluzione tecnologica e delle esigenze produttive e organizzative dell'impresa.

Per quanto riguarda, in particolare, gli Strumenti di lavoro utilizzati da Lavoratrici e Lavoratori, se gli stessi sono forniti dall'azienda (come ad es. la casella di posta elettronica) vengono considerati dotazioni aziendali e per questa ragione controllabili dal datore di lavoro e, ovviamente, inutilizzabili a fini personali.

Con la modernizzazione delle tecniche lavorative e lo sviluppo tecnologico, i controlli a distanza possono risultare, in linea generale, estremamente penetranti nei confronti dei lavoratori, e spingersi fino alla verifica dell'adeguatezza della stessa prestazione lavorativa. Si è reso quindi necessario aggiornare le regole volte alla tutela del lavoratore, contemperando il diritto del datore di lavoro alla tutela dei beni aziendali.

Il Regolamento Generale sulla protezione dei dati UE 2016/679 (GDPR), ha inoltre sancito il principio per il quale **la protezione dei dati personali è un diritto fondamentale dell'individuo**. Più in particolare, il **GDPR** garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

L'ACCORDO DEL 22/5/2014 È STATO QUINDI SOTTOSCRITTO IN UNICREDIT GROUP AL FINE DI OTTEMPERARE A QUANTO RICHIESTO DAL PROVVEDIMENTO DEL GARANTE IN TEMA DI TRACCIAMENTO DELLE OPERAZIONI BANCARIE - SIA DI TIPO DISPOSITIVO CHE DI SEMPLICE VISUALIZZAZIONE – EFFETTUATE UTILIZZANDO INFORMAZIONI CONCERNENTI LA SITUAZIONE ECONOMICA E PATRIMONIALE DEI CLIENTI.

Il Provvedimento del Garante è entrato in vigore il 3 giugno del 2014 e riguarda i rapporti relativi alle **persone fisiche**. In sintesi è stato stabilito che:

- L'Accordo si applica a tutte le Unità Produttive delle aziende del Gruppo UniCredit del perimetro Italia applicanti il CCNL ABI, soggette alle disposizioni del Provvedimento del Garante;
- **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;**
  - **ulteriori informazioni utili solo ad identificare l'operazione (che saranno portate a conoscenza delle lavoratrici/lavoratori**).

- 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;
- Le specifiche tecniche e organizzative approntate e oggetto dell'accordo sottoscritto sono uniformi per tutte le aziende del Gruppo e saranno oggetto di confronto successivo in caso di significative variazioni;
- **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**;
- **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 a personale diversi rispetto al 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**;
- sono altresì previste verifiche periodiche sulla corretta conservazione dei file di log per il periodo" sopra previsto di 24 mesi;
- 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. Inoltre nell'ambito di quanto contrattualmente previsto, possono svolgersi, ove necessario, specifiche attività formative retribuite. In particolare nella prima fase di attuazione del Provvedimento:
    - verrà pubblicata o trasmessa una news con una accurata informativa sul Provvedimento e sugli strumenti utilizzati
    - verrà messo a disposizione di tutto il personale il modulo formativo a fruizione obbligatoria retribuita "Privacy e trattamento dei dati" contenente una specifica sezione sulle prescrizioni e sugli adempimenti del Provvedimento del Garante.

Sul Portale aziendale sono disponibili importanti informazioni sulla Privacy, con particolare riferimento al **Regolamento Generale sulla protezione dei dati UE 2016/679 (GDPR)**, nella sezione:

Strumenti operativi>Strumenti & Applicazioni>Strumenti Personali>Privacy - GPDR