ACCORDO IN MATERIA DI ATTUAZIONE DELL'ART. 4 DELLA LEGGE N. 300/1970

Il giorno 14 ottobre 2021, tramite collegamento virtuale, come previsto dalle attuali disposizioni regolamentari

tra

Allitude S.p.A. (di seguito anche "Allitude" o la "Società")

e

le R.S.A. F.A.B.I., FIRST/CISL, F.I.S.A.C./CGIL e UILCA

assistite dalla Delegazione sindacale di Gruppo F.A.B.I., FIRST CISL, F.I.S.A.C./CGIL, UILCA e UGL CREDITO

(congiuntamente anche le "Parti")

**** *** *** ****

Premesso che:

- l'art. 4 della Legge n. 300/1970, vieta l'uso di impianti audiovisivi per finalità di controllo a distanza dei lavoratori; così come modificato dal D. Lgs. 151/2015, nonché dal D. Lgs. 185/2016, consente l'installazione di impianti audiovisivi ed altri strumenti, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, previo accordo con le RSA.
- Allitude intende dotarsi di impianti audiovisivi, di rilevazione degli accessi ai locali aziendali e di sicurezza logica esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
- Allitude necessita di metodologie cautelative e prudenziali a tutela dei lavoratori interessati e del patrimonio aziendale, adottando un sistema di registrazione/archiviazione dei log di accesso.
- Nel confermare e ribadire l'esclusione della finalità del controllo a distanza dell'attività dei lavoratori, le Parti intendono regolamentare di seguito l'utilizzo dei sistemi di videosorveglianza, di rilevazione degli accessi ai locali aziendali e di sicurezza logica nel rispetto di quanto sancito dall'art. 4 legge 300/70 e dei seguenti principi condivisi:
    - fatti salvi i casi in cui dalla visualizzazione delle immagini e dal trattamento dei dati di accesso ai locali aziendali e di sicurezza logica emergano profili di rilevanza penale, nel qual caso dovranno essere rispettate le procedure e i requisiti di legge, le rilevazioni ottenute in applicazione del presente accordo, dalle quali possa derivare, anche accidentalmente, la possibilità di controllo a distanza dell'attività dei lavoratori, non possono essere utilizzate ai fini disciplinari e per finalità diverse dalla sicurezza del lavoro e per la tutela del patrimonio aziendale;

- I dipendenti verranno tempo per tempo adeguatamente informati e formati sulla raccolta dei dati potenzialmente a loro ascrivibili nonché sui limiti di utilizzo degli strumenti e le sanzioni previste nel caso di violazione di tali limiti;
- i controlli di sicurezza e statistici comunque effettuati, prevedono la raccolta di dati ed eventi in formato anonimo aggregato, riservando la possibilità della correlazione soggettiva solo e nel caso questa sia prevista espressamente da normativa di Legge e/o dalle Autorità italiane ed europee di vigilanza del settore ovvero richiesta dalle autorità giudiziarie in forza di normativa di legge o finalità di sicurezza del lavoro non altrimenti esercitabili;
- le forme di controllo adottate saranno strettamente proporzionate e non eccedenti gli scopi, limitando l'accesso alle rilevazioni ai soli soggetti incaricati, avendo cura di tutelare la riservatezza di quanto raccolto e con il coinvolgimento delle RSA o degli RLS ove non vi fosse una RSA costituita;
- tutte le rilevazioni e i dati verranno conservati per il tempo strettamente necessario previsto dalla normativa di legge tempo per tempo vigente;
- si precisa che tra i trattamenti e i dati conseguentemente raccolti, oggetto del presente accordo, non rientrano i dati biometrici dei dipendenti intesi a identificare in modo univoco una persona fisica;
- fatti salvi i casi di rilevanza penale è vietato l'uso di qualsiasi informazione acquisita sia in formato video che di tracciamento, non connesse allo specifico scopo di tutela e salvaguardia del Patrimonio aziendale o di sicurezza sul lavoro. Inoltre l'azienda non promuoverà verso i dipendenti (comprendendo anche i colleghi di altre strutture del Gruppo eventualmente coinvolti) azioni disciplinari, di rivalsa o di risarcimento nel caso in cui l'Azienda, anche in forma accidentale, venisse a conoscenza di eventuali errori dei dipendenti nell'esecuzione della attività lavorativa.

- Le Società integrate in Allitude rispettivamente a far data dall'1/1/20 (Informatica Bancaria Trentina S.r.l., Servizi Bancari Associati S.p.A., Centro Servizi Direzionali S.r.l.) e dall'1/7/20 (CESVE Servizi Direzionali S.r.l. e Bologna Servizi Bancari S.r.l) hanno precedentemente disciplinato la materia del controllo a distanza attraverso la sottoscrizione di specifici accordi sindacali aziendali.
- In considerazione dei processi di integrazione societaria attualmente in corso e di quanto disposto dal Regolamento UE n. 679/2016 (GDPR) e dal D. Lgs. n. 196/2003 come novellato dal Decreto 101/2018 (c.d. Codice Privacy), si è resa necessaria una complessiva nuova regolamentazione della materia in Allitude.
- Al fine di perseguire gli obiettivi sopra riportati, le Parti manifestano la condivisa volontà di definire principi e linee guida nel rispetto delle esigenze di tutela individuale, di quelle aziendali nonché delle specifiche prerogative sindacali in un accordo complessivo.
- Sulla base di tali principi, l'introduzione di nuove tipologie di impianti e/o apparecchiature e gli interventi che si renderanno necessari saranno oggetto di preventiva illustrazione e confronto con le Organizzazioni Sindacali competenti, al fine di verificare l'applicazione dell'art. 4 Legge n. 300/1970 e la coerenza delle scelte adottate con i principi condivisi nelle presenti intese.

Tutto ciò premesso e considerato, si conviene quanto segue:

1. la premessa forma parte integrante e sostanziale del presente Verbale di Accordo (di seguito anche l'"Accordo");
2. dalla data di sottoscrizione, l'Accordo sostituisce ogni previgente intesa in materia in Allitude e nelle Società nella stessa incorporate;
3. nel confermare l'esclusione delle finalità di controllo a distanza dello svolgimento dell'attività lavorativa, le Parti intendono regolamentare le seguenti materie:

    A. sistemi di videosorveglianza;

    B. sistemi di controllo accesso fisico ad aree aziendali;

    C. controlli di sicurezza logica.

**** *** *** ****

A. SISTEMI DI VIDEOSORVEGLIANZA

L'ubicazione, l'installazione e l'utilizzo degli impianti di videosorveglianza, anche dotati di videoregistrazione nel rispetto delle normative tempo per tempo vigenti in materia, sono finalizzati alla tutela della sicurezza, del patrimonio aziendale e alla prevenzione dei reati, restando esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dei lavoratori.

Al fine di assicurare maggior grado di effettività alle tutele disposte per i lavoratori e del pubblico saranno garantite idonee misure per proteggere i dati di videosorveglianza per evitare che le immagini possano essere diffuse a persone non autorizzate. A questo riguardo l'azienda dovrà garantire che l'accesso sia limitato e tracciato. Qualora per esigenze operative e di sicurezza la videosorveglianza dovesse essere svolta da società esterna, essa dovrà essere appositamente incaricata e informate preventivamente le RSA; è altresì vietata la registrazione audio.

Le telecamere saranno posizionate utilizzando un angolo di visuale necessario allo scopo prefissato in modo tale da salvaguardare, sia all'interno che all'esterno, il rispetto delle prescrizioni dettate dalle normative vigenti. Saranno comunque al di fuori del campo di registrazione, le postazioni di lavoro, salvo casi particolari che saranno eventualmente oggetto di specifico accordo.

Le telecamere hanno le caratteristiche tecniche indicate nell'Allegato 1.

L'impianto di videosorveglianza si compone delle telecamere dislocate sugli edifici di Allitude, come graficamente rappresentato nelle piante allegate (Allegato 2 – visualizzabile presso la sede aziendale). L'allegato comprensivo degli impianti delle sedi territoriali sarà integrato successivamente dopo gli esiti del processo di revisione e armonizzazione in corso, al termine del quale verrà data comunicazione alle RSA.

Ulteriori telecamere potranno essere installate, ricorrendone i presupposti e nel rispetto delle previsioni di legge e del presente Accordo, previa sottoscrizione di specifici accordi con le RSA, che costituiranno Allegati all'Accordo medesimo.

Il trattamento dei dati personali avverrà nel rispetto della normativa vigente in materia di Protezione dei dati personali.

Ai sensi e per gli effetti di quanto previsto dal D. Lgs. n. 196/2003 ss.ii.mm. ("Codice Privacy") e dal Regolamento UE n. 679/2016 ("GDPR"), Allitude provvederà:

I. ad informare tutto il personale, anche mediante l'affissione di appositi cartelli informativi relativi alle aree ed ai locali aziendali soggetti a videosorveglianza;
II. a rendere disponibile copia del presente accordo, integrata con i nominativi dei soggetti abilitati a utilizzare l'impianto e le relative modalità;
III. alle prescritte informative nei confronti degli appaltatori e del personale di questi ultimi che abitualmente svolgono la propria attività lavorativa presso le sedi della Società.

Ai soli fini della tutela delle persone e del patrimonio aziendale, le immagini sono registrate su supporto magnetico/elettronico, conservato dalla Società nel rispetto di rigorose misure di sicurezza (ad esempio in forma criptata) che garantiscano l'impossibilità da parte dei soggetti non autorizzati di accedervi. Le immagini registrate sono mantenute per un periodo di tempo massimo di una settimana, nel rispetto di quanto previsto dalla normativa sulla protezione dei dati personali, dopodiché verranno cancellate automaticamente.

Solamente su richiesta delle autorità giudiziarie e/o di polizia e in relazione esclusivamente alle attività investigative, le immagini registrate potranno essere conservate per un periodo più lungo.

Ai fini di tutela dei dipendenti, le RSA costituite o in caso di loro assenza l'RLS avranno facoltà di verificare il corretto utilizzo dell'impianto di videosorveglianza. Il datore di lavoro deve nominare per iscritto - rendendo noti di volta per volta i nominativi - i responsabili e gli incaricati del trattamento delle immagini, che devono essere appositamente formati sulle modalità di trattamento dei dati.

La visualizzazione delle immagini in caso di necessità di tutela delle persone e del patrimonio aziendale potrà essere effettuata esclusivamente dal Responsabile dell'Ufficio Supporto Logistico - Operativo appositamente individuato ai fini del presidio, congiuntamente con l'incaricato alle attività di verifica ed in presenza delle RSA, ovvero di un RSA delegato, ovvero in mancanza di RSA costituite del RLS.

Le immagini registrate potranno essere esaminate solo nei casi sopra contemplati e potranno essere esportate su supporto fisso (in questa fattispecie solo in situazione di eventi criminosi) esclusivamente in presenza delle RSA, ovvero di un RSA delegato, ovvero in mancanza di RSA costituita del RLS. Analoga informativa dovrà essere attivata automaticamente in qualsiasi caso di accesso ai dati registrati o all'archivio dei log.

L'accesso al sistema è consentito al Responsabile dell'Ufficio Supporto Logistico - Operativo e, ove necessario, ad eventuali suoi collaboratori tempo per tempo specificamente incaricati, solo per attività di "application management" (configurazione, parametrizzazione, verifica e test del sistema); sono previsti diversi livelli di accesso al sistema che contemplano anche l'accesso per interventi di manutenzione, gestione e verifiche sulla funzionalità.

L'accesso al server in "modalità operatore guardia" è definito per il personale che svolge il servizio di vigilanza presso la postazione di guardia di Via Segantini, Trento. Questo profilo

permette l'accesso in modalità live (non alle registrazioni) a tutte le telecamere dell'azienda con esclusive finalità di sicurezza.

L'accesso al server in "modalità operatore reception" è definito per il personale che svolge il servizio di accoglienza presso la reception di Via Aconcio - Trento e presso i Poli per i quali sarà successivamente valutato l'allestimento del servizio di accoglienza dandone comunicazione preventiva alle Organizzazioni Sindacali. Esso consente la visibilità in modalità live (non alle registrazioni) di un sottoinsieme ristretto di telecamere strettamente funzionale allo svolgimento del servizio di portierato.

In presenza di modifiche/integrazioni all'impianto di videosorveglianza, effettuate sempre nel rispetto delle finalità descritte, Allitude fornirà idonea informativa alle R.S.A. firmatarie del presente accordo.

B. SISTEMI DI CONTROLLO ACCESSO FISICO AD AREE AZIENDALI

Le finalità dell'impianto a tecnologia RFID cui sono collegati i terminali che consentono l'apertura dei varchi di accesso, sono quelle di proteggere le persone, le attività e il patrimonio aziendale anche nell'interesse delle società clienti, nonché per la prevenzione di atti criminosi e per disporre di strumenti idonei a verificare e/o registrare la presenza di personale all'interno di tutte le sedi nel rispetto delle norme tempo per tempo vigenti in materia. L'accesso potrà avvenire mediante l'utilizzo di badge o altro strumento utile anche ai fini della registrazione dell'orario di lavoro.

L'impianto è composto da lettori RFID posizionati in prossimità dei varchi di accesso alle sedi di Allitude e da un applicativo software che comprende le funzionalità di impostazione, configurazione, parametrizzazione, personalizzazione e operatività dell'impianto a tecnologia RFID.

I lettori RFID sono posizionati come risulta dalle planimetrie allegate al presente accordo di cui costituiscono parte integrante (Allegato 3 – visualizzabile presso la sede aziendale).

I lettori RFID generano un log degli accessi effettuati che viene conservato su DB locale presente sugli apparati che gestiscono il controllo accessi.

L'accesso al server ed all'applicazione in "modalità amministratore" è riservato al personale dell'Ufficio Supporto Logistico - Operativo. Solo gli utenti espressamente autorizzati hanno accesso ai log e possono effettuare estrazioni solo ed esclusivamente in occasione di audit esterni che periodicamente vengono svolti su incarico scritto di banche clienti o società di certificazione, in occasione di accertamenti legati agli incidenti di sicurezza informatica o su richiesta delle autorità giudiziarie e/o di polizia.

L'accesso in "modalità operatore guardia" è definito per il personale che svolge il servizio di vigilanza presso la postazione di guardia di Via Segantini, Trento, che dispone di privilegi limitati alla gestione delle tessere sostitutive e alla visibilità di pannelli sinottici mediante i quali sono eseguite operazioni sui sistemi anti intrusione con i quali il controllo accessi è interfacciato. Gli operatori non hanno accesso ai log sui transiti dai varchi, né ad altre tipologie.

Un'altra tipologia di profilo operativo è assegnata al personale incaricato della Segreteria generale di Allitude, che svolge le attività di aggiornamento dell'anagrafica (inserimento, cancellazione) e assegnazione dei profili autorizzativi, gestendo le richieste all'interno del processo di assegnazione standard aziendale. Anche questo tipo di profilo non ha visibilità dei log.

In ogni caso, i dati raccolti devono essere protetti con misure di sicurezza tecniche (ad esempio credenziali di autenticazione idonee), organizzative e preventive che abbattano i rischi di distruzione, perdita e accesso non autorizzato dei dati.

La retention dei log è di 6 mesi. Il sistema svolge automaticamente l'eliminazione dei log, per conservare solo una finestra temporale di 6 mesi.

C. CONTROLLI DI SICUREZZA LOGICA

Ai dipendenti, per rendere la propria prestazione lavorativa, sono forniti strumenti informatici che comportano il ricorso a procedure di identificazione, abilitazione all'accesso e tracciatura delle attività che generano tracce log soggette a controlli di sicurezza e a diverse normative.

In particolare, gli istituti operanti nell'ambito dei servizi bancari sono sottoposti a obblighi normativi che richiedono il monitoraggio, anche attraverso l'analisi di log e tracce di audit, di accessi, operazioni e altri eventi, al fine di garantire la sicurezza delle informazioni e delle risorse informatiche, la prevenzione e la gestione degli incidenti di sicurezza, nonché prevenire il trattamento illegittimo e la circolazione delle informazioni personali dei clienti. Al riguardo, è prescritto lo stretto controllo delle attività degli amministratori di sistema e altri utenti privilegiati. Di seguito le principali normative e standard di settore che prescrivono specifici obblighi di tracciamento, monitoraggio e analisi delle attività degli utenti e relativi log:

- "Disposizioni di vigilanza per le banche" – Circolare Banca d'Italia n. 285 del 17 dicembre 2013 e successivi aggiornamenti;
- D. Lgs. 30 giugno 2003, n.196 Codice in materia di protezione dati personali e successive modifiche e integrazioni;
- Provvedimento del 27 novembre 2008 in materia di Amministratori di sistema come modificato dal Provvedimento del 25 giugno 2009 (c.d. "Garante 1");
- Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie del 12 maggio 2011 (c.d. "Garante 2");
- General Data Protection Regulation (EU) n. 2016/679;
- Direttiva PSD2 – Payment Service Directive II – 2015/2366 (UE);
- PSD2 – Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2);
- Orientamenti EBA sulla sicurezza dei pagamenti via internet.

Il monitoraggio di eventi rilevanti sulle risorse informatiche e sulle informazioni personali dei clienti è peraltro conditio sine qua non per l'adesione a circuiti internazionali e standard di settore quali ad esempio Payment Card Industry Data Security Standard -PCI DSS (v. 3.2.1) e SWIFT.

Il provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27/11/2008 del Garante per la protezione dei dati personali (in seguito "Garante 1") richiede l'adozione di idonee modalità di registrazione degli accessi logici ("autenticazione informatica") ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

Le registrazioni ("access log") devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste e devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate. Le parti ritengono importante l'introduzione di procedure che, anche attraverso alert, avvisino l'operatore che in modo involontario operi non in aderenza alla normativa in materia

Il provvedimento "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie" n. 192 del 12/05/2011 del Garante per la protezione dei dati personali" (in seguito anche "Garante 2"), prescrive specifici obblighi al fine di un controllo efficace e dettagliato delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari.

Tutti i presidi di sicurezza informatica approntati sono quindi finalizzati al rispetto della normativa di settore per il contrasto delle minacce di cybersecurity, e producono informazioni per una continua individuazione di eventi anomali ed incidenti.

Tali informazioni vengono prodotte da:

- Sistemi Operativi client e server, applicazioni e servizi.
- Apparati per la difesa perimetrale: Firewall, Web application Firewall, Proxy di navigazione, Intrusion detection and prevention systems, Cloud Access Security Broker, Antivirus di navigazione, Data loss prevention, Content filtering, Application filtering, Sandbox.
- Soluzioni per la protezione degli end point: Endpoint Detection and Response, Antimalware, Anti Advanced Persistent Threat, Personal Firewall, Sandbox, Mobile device management.
- Soluzioni per la tracciatura degli accessi: Identity & Access Management.
- Soluzioni per il contrasto delle frodi: Behavior Analysis, Transaction monitoring.
- Soluzioni per la formazione continua e personalizzata del personale sulle principali minacce cyber.

Per perseguire il contrasto dei fenomeni di Cybersecurity, le informazioni prodotte vengono analizzate e correlate sia manualmente che da sistemi automatici specializzati come sistemi di LOG Management, SIEM (Security Information Event Management) che, a fronte di regole predefinite o da meccanismi di Artificial Intelligence, producono allarmi che sono analizzati da personale identificato e specializzato, appartenente al Servizio Cyber Security Operations e relativi correlati fornitori al fine di garantire un presidio 24h/24h 365 giorni anno.

La gestione sistemistica dei dispositivi ospitanti le informazioni è inoltre consentita, garantendo il principio del privilegio minimo, anche al personale sistemistico identificato e denominato (c.d. Amministratori di Sistema).

L'accesso a tali informazioni può inoltre essere concesso anche agli esecutori di controlli di primo livello (es. per fini di rispetto privacy), alle funzioni di controllo aziendali e di gruppo, e alle autorità giudiziarie o di vigilanza.

L'accesso alle informazioni e agli apparati avviene mediante processi autorizzativi codificati, tracciati e verificati periodicamente.

Le politiche di conservazione dei log seguono i dettami normativi e prevedono generalmente la conservazione per un tempo non superiore ai 24 mesi.

**** *** *** ****

In ogni caso, i dati raccolti devono essere protetti con misure di sicurezza tecniche (ad esempio credenziali di autenticazione idonee), organizzative e preventive che abbattano i rischi di distruzione, perdita, accesso non autorizzato dei dati.

La richiesta di attivazione della procedura di verifica potrà essere effettuata anche dal singolo dipendente avanzandone richiesta scritta motivata, fermo il diritto del lavoratore interessato di farsi assistere da un RSA, ovvero in mancanza da un dirigente sindacale delegato.

Nel caso in cui da qualsiasi informazione acquisita sia in formato video che di tracciamento emergano profili di rilevanza penale relativamente al comportamento di un dipendente, la struttura aziendale che ne viene a conoscenza informa con immediatezza l'Ufficio Gestione Risorse Umane per le opportune valutazioni e, se dai medesimi comportamenti aventi rilevanza penale emergesse anche una rilevanza ai fini disciplinari, il dipendente interessato potrà aver accesso alle rilevazioni video o di tracciamento avvalendosi anche dell'assistenza di un rappresentante della Organizzazione Sindacale alla quale aderisce o conferisce mandato.

In presenza di modifiche/integrazioni all'impianto di tracciamento delle attività, effettuate sempre nel rispetto delle finalità descritte, verrà tempestivamente fornirà idonea informativa alle R.S.A. firmatarie del presente accordo.

L'azienda fornirà alle RSA il documento di valutazione di impatto sulla protezione dei dati (cd. DPIA) ed eventuali successive modifiche. Qualora l'Azienda nel redigere la valutazione di impatto sulla protezione dei dati (cd. DPIA) rilevi eventuali rischi per gli utenti, il Titolare del trattamento darà tempestiva informativa alle RSA sulle concrete misure tecnico organizzative per ridurli.

Le caratteristiche tecniche degli impianti di videosorveglianza, sistemi di controllo accesso fisico e controlli di sicurezza logica, la conservazione dei files video e dei registri dei log, nonché le procedure tecniche seguite nelle fasi di videoregistrazione e estrazione/duplicazione e visualizzazione delle registrazioni video o dei tracciamenti, in qualsiasi forma fin qui disciplinata, sono dettagliate nella normativa aziendale tecnica e procedurale di riferimento, ispirata alle linee guida del presente Accordo e ad esso conforme.

Le OO.SS. monitoreranno che il ricorso ai sistemi di Intelligenza Artificiale tecnici e informatici oggetto del presente accordo, si sviluppi in equilibrio con la valorizzazione delle persone e delle professionalità, nonché con la tenuta dei livelli occupazionali. In nessun caso

potranno essere visualizzati i tempi di permanenza nelle varie attività cui il dipendente è adibito durante il proprio orario di lavoro, nonché, altre forme di visualizzazione indebita dei predetti tempi, compreso l'utilizzo ai fini della valutazione della prestazione professionale.

Le Parti firmatarie si danno reciprocamente atto che qualora dovessero intervenire significative modifiche all'impianto normativo, legale e/o di settore riguardante le materie disciplinate dal presente accordo si incontreranno per concordare gli adattamenti e gli interventi che si dovessero rendere necessari, nonché, in qualsiasi momento a richiesta di una delle Parti per la valutazione congiunta circa lo stato di applicazione di quanto previsto e fin qui concordato.

Si allegano:

1) Caratteristiche tecniche telecamere;
2) Ubicazione telecamere (visualizzabile presso la sede aziendale);
3) Planimetrie lettori RFID (visualizzabile presso la sede aziendale);

Letto, accettato e sottoscritto.

p. Allitude Spa

_____

p. le OOSS

F.A.B.I. _____

FIRST CISL _____

F.I.S.A.C. CGIL _____

U.I.L.C.A. _____

UGL CREDITO _____