# ACCORDO QUADRO

**per la disciplina dell'attuazione dell'art. 4 della Legge 300/1970 per i dipendenti delle BCC – CR – RAIKA e delle Aziende del Gruppo Bancario Cooperativo Cassa Centrale Banca**

Il giorno 5 maggio 2026 presso la sede di Cassa Centrale Banca,

tra

**CASSA CENTRALE BANCA - CREDITO COOPERATIVO ITALIANO SPA** (di seguito anche **"Cassa Centrale"**), nella qualità di **CAPOGRUPPO DEL GRUPPO BANCARIO COOPERATIVO CASSA CENTRALE BANCA**;

E

La **Delegazione Sindacale di Gruppo**, costituita ai sensi dell'art. 11 bis CCNL, così composta per le seguenti OO. SS.:

**FABI**

**FIRST CISL**

**FISAC CGIL**

**UGL Credito**

**UIL C.A.**

## Premesso che

a) L'art. 4 della Legge n. 300/1970, vieta l'uso di impianti audiovisivi per finalità di controllo a distanza delle lavoratrici e 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.
b) L'art. 11 bis 4 comma quinto capoverso del CCNL vigente consente alla Delegazione Sindacale di Gruppo di "definire accordi quadro di interesse

collettivo che riguardino contestualmente tutte o parte delle Banche di Credito Cooperativo/Casse Rurali ed Artigiane aderenti e le Aziende facenti parte di Gruppo Bancario Cooperativo di cui al comma 1, lettera b) dell'articolo 8, che compongono il Gruppo Bancario Cooperativo interessato; gli accordi eventualmente raggiunti in tale sede potranno essere recepiti nelle Aziende aderenti al Gruppo previo confronto con le Rappresentanze Sindacali Aziendali ivi costituite da concludersi entro 20 giorni". Detto termine, non a carattere perentorio, decorre dalla data di consegna della bozza della valutazione di impatto sulla protezione dei dati (DPIA).

c) In tale contesto, le Parti intendono definire un accordo quadro di riferimento in materia di controllo a distanza, in conformità delle disposizioni normative e regolamentari vigenti che sia adottabile dalla generalità delle BCC- CR e aziende del Gruppo Bancario Cassa Centrale Banca.

d) Le Parti condividono che l'adozione di impianti audiovisivi, di rilevazione degli accessi ai locali aziendali e di sicurezza logica deve avvenire esclusivamente per specifiche e limitate esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, secondo presupposti di stretta necessità, pertinenza e proporzionalità e nell'integrale rispetto della privacy e dei diritti fondamentali delle lavoratrici e dei lavoratori, con riferimento sia alla tipologia ed alla quantità dei dati da acquisire, sia alla custodia, alla gestione e all'utilizzo dei dati effettivamente acquisiti. La responsabilità di quanto sopra riportato, con riferimento ai dati, incombe sulla BCC/Azienda del Gruppo Bancario Cassa Centrale Banca.

e) le Parti richiamano la necessità dell'adozione di metodologie cautelative e prudenziali a tutela delle lavoratrici e dei lavoratori interessati e del patrimonio aziendale, utilizzando un sistema di registrazione/archiviazione dei log di accesso, strutturata secondo un approccio basato sul rischio e calibrata in base al livello di criticità delle informazioni stesse, determinato dai requisiti di riservatezza, integrità e disponibilità, al fine di implementare misure di rilevamento efficaci ed efficienti che ottimizzino le risorse impiegate e rispettino i principi di necessità, pertinenza e proporzionalità e i diritti di cui al precedente punto d) della premessa.

f) Nel confermare e ribadire l'esclusione della finalità del controllo a distanza dell'attività delle lavoratrici e dei lavoratori, le Parti intendono regolamentare l'utilizzo dei sistemi di videosorveglianza, di rilevazione degli accessi ai locali aziendali e di sicurezza logica presso le BCC- CR e aziende del Gruppo nel rispetto di quanto sancito dall'art. 4 legge 300/70 nonché successive modifiche e integrazioni e dei seguenti principi condivisi:

- Le risultanze della videosorveglianza, dei sistemi di controllo accessi e dei sistemi di sicurezza logica sono trattate esclusivamente per le finalità e per la tutela dei diritti di cui al punto d), nel rispetto dei principi di necessità, pertinenza, proporzionalità, minimizzazione e limitazione della conservazione. Esse non sono utilizzabili per finalità di controllo dell'attività lavorativa o di valutazione della prestazione. L'eventuale utilizzo a fini disciplinari potrà avvenire solo ed esclusivamente a fronte di uno specifico e grave fatto posto in essere con comportamento doloso, idoneo a integrare ipotesi di reato connesse ad attività fraudolente tali da determinare un pregiudizio al patrimonio o alla sicurezza.

  In tali casi, il datore di lavoro può procedere all'estrazione e alla conservazione delle sole evidenze strettamente pertinenti all'evento, secondo procedure formalizzate che prevedano specifica autorizzazione, tracciamento degli accessi e limitazione dei soggetti abilitati, nel rispetto della normativa vigente in materia di protezione dei dati personali e dell'informativa resa ai lavoratori;
- I dipendenti verranno preventivamente e adeguatamente informati e formati sulla raccolta dei dati potenzialmente a loro ascrivibili, nonché sui limiti di utilizzo degli strumenti e le sanzioni previste dalla legge nel caso di violazione di tali limiti. Tale formazione/informazione sarà oggetto di preventivo confronto all'interno delle procedure contrattualmente previste;
- i controlli di sicurezza e statistici comunque effettuati, fermo quanto indicato sopra ai fini disciplinari, prevedono la raccolta di dati ed eventi solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori. La possibilità della correlazione soggettiva è dunque

riservata esclusivamente al caso in cui 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;

- RSA/RLS potranno effettuare verifiche a posteriori sull'operato svolto da parte della Funzione aziendale competente richiedendo log a campione relativamente a specifici apparati, inoltrando apposita e-mail all'Ufficio/Figura appositamente incaricato/a. L'azienda dovrà, entro 5 gg dalla richiesta, dare soddisfazione alla richiesta medesima. A fronte di contenzioso/i disciplinare/i nelle fattispecie di cui al primo alinea, le RSA/RLS potranno verificare le modalità e le temporalità di accesso e di raccolta dati effettuate dall'ufficio preposto, sui dati del dipendente oggetto del contenzioso medesimo;
- le forme di controllo adottate, l'acquisizione e il trattamento dei dati, saranno limitati, pertinenti, proporzionati e non eccedenti gli scopi strettamente inerenti al rapporto di lavoro, oltre che rispettosi dei diritti di cui al punto d) della premessa, limitando l'accesso alle rilevazioni ai soli soggetti incaricati, avendo cura di tutelare la riservatezza di quanto raccolto. Le lavoratrici e i lavoratori coinvolti potranno chiedere l'assistenza di un rappresentante della Organizzazione Sindacale alla quale aderiscono o conferiscono mandato senza con ciò precludere o interferire con le attività e le tempistiche di indagine da parte delle Autorità;
- Tutte le rilevazioni, i dati contenuti nei log dovranno essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di limitazione della conservazione) e comunque per un periodo non superiore a quanto previsto dalla normativa di legge e secondaria tempo per tempo vigenti. In base al principio di responsabilizzazione l'azienda deve essere sempre in grado di motivare il periodo di conservazione definito. L'organizzazione sindacale potrà chiedere evidenza della documentazione atta a comprovare le scelte alla base della definizione del periodo di conservazione;

- Sono vietati l'acquisizione e l'uso di qualsiasi informazione non connessa allo specifico scopo di stretta tutela e salvaguardia del patrimonio aziendale o di sicurezza sul lavoro così come disciplinato dal presente accordo;
- 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 la corretta applicazione e la coerenza delle scelte adottate con i principi condivisi nelle presenti intese in virtù di quanto disposto dall'art. 4 Legge n. 300/1970.

Qualora intervengano rilevanti modifiche e/o integrazioni degli impianti audiovisivi, di rilevazione degli accessi ai locali aziendali e di sicurezza logica, per effetto di processi di accentramento di gruppo, e ferme le necessità di adeguamento dei verbali di accordo sottoscritti, di cui all'allegato A, la Capogruppo informerà preventivamente la delegazione sindacale di Gruppo anche al fine, qualora necessario, dell'integrazione o della modifica del presente accordo quadro.

Considerato:

quanto disposto dal Regolamento UE n. 679/2016 (GDPR) e dal D. Lgs. n. 196/2003 come novellato dal D. Lgs. n.101/2018 (c.d. Codice Privacy) e dal Regolamento europeo 1689/2024, dalla Legge 132/2025 e dalle ulteriori previsioni legislative in quanto applicabili.

Tutto ciò premesso e considerato, si conviene quanto segue:

1. Le premesse costituiscono parte integrante e sostanziale del presente accordo.
2. Le parti condividono che costituisce presupposto formale e sostanziale per l'avvio di ogni procedura di confronto aziendale ex art. 4, L. 300/1970 la previa illustrazione e consegna alle Organizzazioni Sindacali, da parte del datore di lavoro, della bozza della Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

di cui all'art. 35 del GDPR (Regolamento UE 2016/679), che costituirà la base di partenza della valutazione negoziale e di cui l'eventuale accordo sindacale dovrà costituire parte integrante, insieme agli allegati tecnici che descriveranno gli specifici sistemi e processi di acquisizione e gestione dei dati e gli strumenti di tutela dei diritti fondamentali. Le parti si danno atto e concordano che la effettiva consegna della DPIA conforme alla bozza, illustrata alla RSA, costituisce condizione di efficacia sospensiva dell'accordo sindacale.

3. Le parti condividono la bozza di accordo aziendale di cui all'allegato A, che potrà essere recepita in ciascuna delle AZIENDE/CRA/BCC/RAIKA del Gruppo Cassa Centrale Banca Credito Cooperativo Italiano previo confronto con le rispettive RSA ivi costituite, da attivarsi alla consegna della bozza di valutazione di impatto sulla protezione dei dati (DPIA), secondo quanto previsto dalla lettera b delle premesse".
4. Le parti monitoreranno l'attuazione di tale accordo quadro nelle AZIENDE/CRA/BCC/RAIKA del Gruppo e, qualora emergessero criticità, attiveranno la procedura di cui all'art. 17 del CIG. In ogni caso, copia dell'accordo collettivo aziendale sottoscritto dovrà essere inviata alla Capogruppo e alla Delegazione sindacale di gruppo.
5. Il presente accordo quadro sarà allegato al contratto integrativo di gruppo.

Letto, accettato e sottoscritto.

Trento, 5 maggio 2026

| | |
|---|---|
| Per Cassa Centrale Banca – Credito Cooperativo Italiano SpA | Per la Delegazione Sindacale di Gruppo Bancario Cooperativo Cassa Centrale Banca |
| _____ | FABI<br>_____ |

FIRST - CISL

_____

FISAC – CGIL

_____

UGL CREDITO

_____

UILCA

_____

**ALLEGATO A**

**VERBALE DI ACCORDO EX ART. 4 LEGGE 300/70 IN MATERIA DI CONTROLLO A DISTANZA**

**TRA**

**CRA/BCC/RAIKA/AZIENDA ……..**

**E**

**LE RRSSA ……**

**PREMESSO CHE**

- Le Parti, nel richiamare integralmente quanto definito nell'accordo quadro del ~~data~~ ……2026 tra Cassa Centrale Banca - Credito Cooperativo Italiano Spa, in qualità di Capogruppo del Gruppo Bancario Cooperativo Cassa Centrale Banca, e la Delegazione Sindacale di Capogruppo, ai sensi dell'art 4 della Legge 300/1970 in materia di controllo a distanza, intendono sottoscrivere il seguente accordo.
- Costituisce presupposto formale e sostanziale per l'avvio del confronto aziendale ex art. 4, L. 300/1970 la previa illustrazione e consegna alle Organizzazioni Sindacali, da parte del datore di lavoro, della bozza della Valutazione d'Impatto sulla Protezione dei Dati (DPIA) di cui all'art. 35 del GDPR (Regolamento UE 2016/679), che costituirà la base di partenza della valutazione negoziale di cui al presente accordo, e dovrà costituire parte integrante, insieme agli allegati tecnici che descriveranno gli specifici sistemi e processi di acquisizione e gestione dei dati e gli strumenti di tutela dei diritti fondamentali. Le parti, così come espressamente sancito nell'accordo quadro di riferimento sottoscritto a livello di Gruppo il 5 maggio 2026, si danno atto e concordano che la effettiva consegna della DPIA, così come illustrata alla RSA costituisce condizione di efficacia sospensiva del presente accordo sindacale.

Tutto ciò premesso, si conviene quanto segue:

1. la premessa forma parte integrante e sostanziale del presente Verbale di Accordo (di seguito detto anche" Accordo");
2. 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. controlli di sicurezza sul sistema informativo;
   C. sistemi di controllo degli accessi fisici ad aree aziendali [Eventuale].

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

**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 delle lavoratrici e dei lavoratori.

Le risultanze della videosorveglianza, dei sistemi di controllo accessi e dei sistemi di sicurezza logica sono trattate esclusivamente per le finalità di cui al punto d) delle premesse dell'Accordo Quadro, nel rispetto dei principi di necessità, proporzionalità, minimizzazione e limitazione della conservazione. Esse non sono utilizzabili per finalità di controllo dell'attività lavorativa o di valutazione della prestazione. L'eventuale utilizzo a fini disciplinari potrà avvenire solo ed esclusivamente a fronte di uno specifico e grave fatto posto in essere con comportamento doloso, idoneo a integrare ipotesi di reato connesse ad attività fraudolente tali da determinare un pregiudizio al patrimonio o alla sicurezza.

In tali casi, il datore di lavoro può procedere all'estrazione e alla conservazione delle sole evidenze strettamente pertinenti all'evento, secondo procedure formalizzate che prevedano specifica autorizzazione, tracciamento degli accessi e limitazione dei soggetti abilitati, nel rispetto della normativa vigente in materia di protezione dei dati personali e dell'informativa resa ai lavoratori.

Fermo restando le finalità di cui appena innanzi - eccezion fatta per i casi di mera visualizzazione delle immagini in tempo reale da parte del personale appositamente designato per iscritto dalla BCC/CRA/RAIKA/Azienda - al fine di assicurare maggior grado di effettività alle tutele disposte per le lavoratrici e i lavoratori e per il pubblico, saranno garantite idonee misure per proteggere i dati di videosorveglianza, per evitare che le immagini salvate possano essere diffuse a persone non autorizzate. A questo riguardo, l'azienda garantisce che l'accesso ai dati salvati 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 si dovranno informare 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 oggetto di valutazione preventiva e confronto con le RSA al fine di tutelare i reciproci interessi e di garantire la privacy e i diritti fondamentali delle lavoratrici e dei lavoratori adottando, in ogni caso, sistemi di oscuramento della postazione lavorativa. In ogni caso, le immagini che possano contenere anche incidentalmente l'inquadratura di postazioni di lavoro, potranno essere utilizzate dalla Banca solo in caso di eventi criminosi, per mettere le stesse a disposizione dell'autorità di polizia e/o dell'autorità giudiziaria dietro specifica richiesta. Verranno oscurate le immagini non necessarie ai fini richiesti dalle autorità per le relative indagini. Resta salvo il diritto del dipendente di richiedere l'accesso alle immagini che lo riguardano.

Le telecamere hanno le caratteristiche tecniche indicate nell'apposito documento allegato al presente accordo e reperibile nella intranet aziendale, all'indirizzo www……. (valutare se la BCC archivi in intranet) oppure (indicare ove possibile reperire il documento).

L'impianto di videosorveglianza si compone delle telecamere dislocate negli edifici della BCC/CRA/RAIKA/Azienda, così come graficamente rappresentato nelle piante allegate al presente accordo.

Ulteriori telecamere potranno essere eventualmente installate, ricorrendone i presupposti e nel rispetto delle previsioni di legge e del presente Accordo, previa verifica e adeguamento del presente accordo.

Il trattamento dei dati personali avverrà nel rispetto della normativa vigente in materia di Protezione dei dati personali e secondo i principi individuati nell'Accordo quadro sottoscritto il 5 maggio 2026.

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") dal Regolamento europeo 1689/2024, dalla Legge 132/2025 e dalle ulteriori previsioni legislative in quanto applicabili anche ai sistemi di videosorveglianza, la BCC/CRA/RAIKA/Azienda provvederà:

I. ad informare tramite canali ufficiali tutto il personale, interno ed esterno 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, prima dell'attivazione del medesimo impianto.

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, e in ogni caso nel rispetto di quanto previsto dalla normativa sulla protezione dei dati personali, dopodiché verranno cancellate.

Solamente nei casi di contenzioso disciplinare a fronte di uno specifico e grave fatto posto in essere con comportamento doloso, idoneo a integrare ipotesi di reato connesse ad attività fraudolente tali da determinare un pregiudizio al patrimonio o alla sicurezza, ovvero su richiesta dell'Autorità Giudiziaria e/o delle forze dell'ordine e in relazione esclusivamente alle attività investigative, e nei casi consentiti dalla normativa vigente, le immagini registrate potranno essere conservate per il tempo strettamente necessario alle verifiche. In difetto, le immagini sono cancellate automaticamente.

Ai fini di tutela delle lavoratrici e dei lavoratori, le RSA costituite e l'RLS avranno facoltà di verificare, anche individualmente, il corretto utilizzo dell'impianto di videosorveglianza. Il datore di lavoro deve nominare per iscritto - rendendo noti di volta per volta i nominativi anche alle RSA e alle RLS - i responsabili e gli incaricati del trattamento delle immagini, che devono essere appositamente formati sulle modalità di trattamento dei dati. All'atto della sottoscrizione del presente accordo collettivo l'Azienda dichiara che la/il responsabile del predetto trattamento è ……..

La responsabilità della visualizzazione, dell'estrapolazione e della trasmissione delle immagini sarà un'attività esclusiva dell'Ufficio_____ [*Nota: indicare l'ufficio di competenza*] ovvero del diverso eventuale Ufficio tempo per tempo incaricato e preventivamente comunicato alle RSA. La visualizzazione, l'estrapolazione e la trasmissione delle immagini dovranno avvenire congiuntamente con la struttura incaricata alle attività di verifica. Le lavoratrici e i lavoratori coinvolti potranno chiedere l'assistenza di un rappresentante dell'Organizzazione Sindacale alla quale aderiscono o conferiscono mandato senza con ciò precludere o interferire con le attività e le tempistiche di indagine da parte delle Autorità.

L'accesso al sistema è altresì consentito all'ufficio tecnico o società terza [*da individuare*], tempo per tempo specificamente designati, solo per attività di cui al presente accordo. Resta inteso che le Società terze non svolgeranno in ogni caso alcuna attività di controllo a distanza dell'attività lavorativa;

In presenza di modifiche/integrazioni all'impianto di videosorveglianza, effettuate sempre nel rispetto delle finalità descritte, la BCC/CRA/RAIKA/Azienda fornirà idonea informativa preventiva alle R.S.A. per le necessarie implementazioni del presente accordo.

**B. CONTROLLI DI SICUREZZA SUL SISTEMA INFORMATIVO**

Ai dipendenti, per rendere la propria prestazione lavorativa, sono forniti strumenti informatici aziendali 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;
- Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology – ICT) e di sicurezza;
- Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554.

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. 4 e successive) e SWIFT.

Le attuali normative richiedono di fatto per le entità finanziarie di definire, stabilire e implementare un processo di gestione degli incidenti legati alle ICT per rilevare e gestire e notificare gli incidenti legati alle tecnologie della informazione e comunicazione.

Gli enti finanziari devono registrare tutti gli incidenti e le minacce informatiche significative e stabilire procedure e processi adeguati a garantire un monitoraggio,

una gestione e un follow-up coerenti e integrati degli incidenti, per garantire che le cause profonde siano identificate, documentate e affrontate al fine di prevenire il verificarsi di tali incidenti, attraverso:

- predisposizione di meccanismi per individuare tempestivamente attività anomale, problemi di prestazione della rete delle TIC, incidenti ad esse connessi, punti di guasto importanti.
- Meccanismi periodicamente testati e che prevedano molteplici livelli di controllo, definiscano soglie di allarme e criteri per l'avvio dei processi di individuazione degli incidenti e di risposta agli stessi.
- Istituzione di meccanismi di allarme automatico per il personale incaricato della risposta agli incidenti.
- Allocazione di risorse e capacità sufficienti al monitoraggio delle attività degli utenti.
- Predisposizione di indicatori di early warning, con l'impostazione di un sistema di monitoraggio proattivo mirato a prevenire il verificarsi degli incidenti informatici.
- Svolgimento attività di monitoraggio, utilizzando indicatori quantitativi e qualitativi per rilevare casi di utilizzo improprio delle banche dati da parte del personale, interno ed esterno, come previsto dalla normativa di primo e secondo livello tempo per tempo vigenti.

L'azienda assicura quindi che tutti i presidi di sicurezza informatica approntati sono espressamente ed esclusivamente 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, tra cui: 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 tra cui: Endpoint Detection and Response, Antimalware, Anti Advanced Persistent Threat, Personal Firewall, Sandbox, Mobile device management, DNS-layer security.

- Soluzioni per gestione e tracciatura delle identità logiche e dei relativi permessi di accesso ai sistemi e agli applicativi aziendali: Identity & Access Management, Privilege 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.

La conformità alle previsioni di legge dei dispositivi sopra elencati è di esclusiva responsabilità dell'Azienda.

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 di meccanismi di Artificial Intelligence, producono allarmi che sono analizzati da personale identificato e specializzato, appartenente al Servizio Cyber Security Operations di Allitude S.p.a. 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 e del monitoraggio delle attività, anche al personale sistemistico identificato e denominato (c.d. Amministratori di Sistema e Utenti Privilegiati).

L'accesso a tali informazioni, finalizzato alla sicurezza aziendale e a ragioni di compliance, purché avvenga sempre nel rispetto della normativa sulla privacy e delle norme e principi di cui al presente accordo, può inoltre essere concesso anche agli esecutori di controlli, alle funzioni di controllo aziendali e di gruppo, o ad altri soggetti autorizzati, in ogni caso secondo un principio di need to know, con autorizzazioni tracciate e verificate, nonché 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 sono definite in apposito allegato tecnico (retention per categorie), con indicazione delle ragioni (accountability) e sono soggette a riesame periodico, almeno annuale. Resta inteso che le RSA potranno chiedere evidenza della documentazione a supporto delle scelte effettuate da parte datoriale.

## C. SISTEMI DI CONTROLLO DEGLI ACCESSI FISICI AD AREE AZIENDALI [EVENTUALE E DA ADATTARE AL SISTEMA ADOTTATO DA CIASCUNA REALTA' AZIENDALE]

Oggetto della presente norma è l'utilizzo degli impianti che consentono l'apertura dei varchi di accesso. Essi, nel rispetto delle previsioni di cui alle premesse dell'accordo quadro, hanno lo scopo di proteggere le persone, le attività e il patrimonio aziendale anche nell'interesse dei clienti, nonché prevenire gli atti criminosi e per disporre di strumenti idonei a registrare la presenza di personale all'interno di tutte le sedi nel rispetto delle norme tempo per tempo vigenti in materia.

L'impianto, così come identificato nel documento reperibile nella intranet aziendale, all'indirizzo http://_____ ed allegato al presente accordo (anche reperibile attraverso___) è composto…. (*nota da compilare*: *descrivere sommariamente le caratteristiche dell'impianto, es: da lettori RFID posizionati in prossimità dei varchi di accesso alle sedi e da un applicativo software che comprende le funzionalità di impostazione, configurazione, parametrizzazione, personalizzazione e operatività dell'impianto a tecnologia RFID).*

L'accesso al server ed all'applicazione in "modalità amministratore" è riservato a personale dell'Ufficio _____ ovvero del diverso eventuale Ufficio tempo per tempo incaricato e comunicato alle RSA/RLS. Solo gli utenti espressamente autorizzati hanno accesso ai log e possono effettuare estrazioni solo ed esclusivamente in occasione di audit, in occasione di accertamenti legati agli incidenti di sicurezza informatica o su richiesta delle Autorità giudiziarie e/o di polizia.

L'eventuale accesso in "modalità operatore guardia" è definito per il personale che svolge il servizio di vigilanza presso la postazione di guardia di Via _____, ovvero della diversa eventuale postazione, tempo per tempo incaricato e comunicato alle RSA/RLS, che dispone di privilegi limitati alla gestione delle tessere sostitutive e alla visibilità di pannelli sinottici, mediante i quali sono eseguite operazioni sui sistemi antintrusione con i quali il controllo accessi è interfacciato. Gli operatori di guardia non hanno accesso ai log sui transiti dai varchi, né ad altre tipologie. In caso di esternalizzazione del servizio va rivista la valutazione.

Un'altra eventuale tipologia di profilo operativo è assegnata al personale incaricato dell'Ufficio_____ ovvero del diverso eventuale Ufficio tempo per tempo incaricato e comunicato alle RSA/RLS 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 sono 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 conservazione ordinaria dei log di accesso fisico è limitata a 90-180 giorni, con durata definita e motivata in DPIA in funzione del rischio e dell'operatività, e in ogni caso nel rispetto delle prescrizioni di legge e delle Autorità competenti. È esclusa la conservazione generalizzata pluriennale. Solo in presenza di specifici eventi oggetto di contestazione disciplinare a fronte di uno specifico e grave fatto posto in essere con comportamento doloso, idoneo a integrare ipotesi di reato connesse ad attività fraudolente tali da determinare un pregiudizio al patrimonio o alla sicurezza, e/o di accertamenti da parte dell'autorità giudiziaria e/o da organi della polizia giudiziaria per i fini di sicurezza di cui al presente accordo (es. accesso non autorizzato, furto/rapina, danneggiamento), i soli dati pertinenti possono essere 'congelati' e conservati per il tempo strettamente necessario alle verifiche. Il sistema svolge automaticamente l'eliminazione dei log e dei dati di accesso fisico per conservarli solo nelle finestre temporali innanzi richiamate.

Detti dati di accesso non sono utilizzabili per finalità di controllo dell'attività lavorativa, valutazione della prestazione. L'eventuale utilizzo a fini disciplinari potrà avvenire esclusivamente a fronte di uno specifico e grave fatto posto in essere con comportamento doloso, idoneo a integrare ipotesi di reato connesse ad attività fraudolente tali da determinare un pregiudizio al patrimonio o alla sicurezza.

In tali casi, il datore di lavoro può procedere all'estrazione e alla conservazione delle sole evidenze strettamente pertinenti all'evento, secondo procedure formalizzate che prevedano specifica autorizzazione, tracciamento degli accessi e limitazione dei soggetti abilitati, nel rispetto della normativa vigente in materia di protezione dei dati personali e dell'informativa resa ai lavoratori.

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

In ogni caso, l'azienda garantisce che i dati raccolti sono 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.

Il dipendente, che avanzi richiesta scritta motivata, può verificare i dati a lui ascrivibili, fermo il suo diritto di farsi assistere da un RSA, ovvero in mancanza da un dirigente sindacale delegato.

Qualora, a seguito di specifiche anomalie o eventi di sicurezza, si renda necessario procedere all'estrazione e/o correlazione nominativa di immagini o log o degli accessi, la struttura aziendale competente opera esclusivamente secondo le finalità e la procedura previste dal presente accordo (trigger, autorizzazione scritta, tracciamento accessi, minimizzazione).

Ferme restando le competenze delle Autorità e l'inutilizzabilità ai fini disciplinari dei dati acquisiti salvo quanto sopra previsto, il lavoratore interessato è informato senza ritardo compatibile con eventuali esigenze investigative; è garantita la possibilità di assistenza sindacale, senza interferire con le attività e le tempistiche di indagine.

In presenza di modifiche/integrazioni all'impianto di tracciamento delle attività, effettuate sempre nel rispetto delle finalità descritte, l'Azienda fornirà idonea informativa preventiva alle R.S.A. per le necessarie ed eventuali modifiche e implementazioni del presente accordo o per la sottoscrizione di un nuovo accordo.

In nessun caso potranno essere raccolti e utilizzati dati che rilevano i tempi di permanenza nelle varie attività cui il dipendente è adibito durante il proprio orario di lavoro, compreso il loro utilizzo ai fini della valutazione della prestazione professionale.

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

Le Parti firmatarie si danno reciprocamente atto che, qualora dovessero intervenire 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 allega al presente accordo la bozza della Valutazione d'Impatto sulla Protezione dei Dati (DPIA) di cui all'art. 35 del GDPR (Regolamento UE 2016/679), di cui il presente accordo sindacale costituisce parte integrante.

Si allegano inoltre gli allegati tecnici che descrivono gli specifici sistemi e processi di acquisizione e gestione dei dati e gli strumenti di tutela dei diritti fondamentali. Tali documenti costituiscono parte integrante del presente accordo collettivo aziendale.

Le parti ribadiscono le premesse e concordano che la effettiva consegna della DPIA conforme alla bozza previamente illustrata alle RSA, costituisce condizione di efficacia sospensiva del presente accordo.

Letto, accettato e sottoscritto.

La Banca Le RSA

_____ _____