

VERBALE DI INCONTRO

ex art. 11 bis, comma 4, quinto capoverso, del CCNL 11.06.2022 per i quadri direttivi e per il personale delle aree professionali delle BCC/CR

In data 4 dicembre 2023, in presenza e attraverso collegamento telematico con piattaforma Teams,

tra

Iccrea Banca S.p.A. Istituto Centrale del Credito Cooperativo, Capogruppo del Gruppo Bancario Cooperativo Iccrea, nella qualità di Capogruppo

e

la **Delegazione Sindacale di Gruppo**, in rappresentanza delle seguenti OO.SS:

- FABI
- FIRST CISL
- FISAC CGIL
- UGL CREDITO
- UILCA UIL

Premesso che

- In data 18 marzo 2022, la Capogruppo Iccrea Banca S.p.A. ha inviato alla Delegazione Sindacale di Gruppo e alle Segreterie Nazionali delle OO.SS. apposita informativa ai sensi dell'art. 11 bis, comma 4, quinto capoverso, al fine di avviare un confronto per disciplinare in modo quanto più possibile organico, mediante un Accordo Quadro che potrà essere recepito, a seguito di confronto, dalle Società del cd. "Perimetro Diretto"/BCC aderenti e le rispettive RR.SS.AA., la materia della videosorveglianza, del tracciamento delle operazioni bancarie e dell'utilizzo della posta aziendale e di internet;
- le Parti, nella consapevolezza della necessità di adeguare le regolamentazioni aziendali in materia di videosorveglianza e tracciamento delle operazioni bancarie ai cambiamenti che hanno riguardato l'assetto organizzativo del Gruppo e la normativa sopravvenuta in materia di privacy, nel corso dell'anno 2022 hanno avviato un confronto;
- le Parti si sono incontrate, oltre che in data odierna, il 18, 24 gennaio, 30, 31 ottobre, 3, 6 e 22 novembre e il 4 dicembre, pervenendo da ultimo ad una condivisione della disciplina in materia di videosorveglianza delle filiali ai fini di prevenzione antirapina e tutela del patrimonio aziendale e in materia di tracciamento delle operazioni bancarie;
- le Parti non hanno invece avviato il confronto sull'accordo in materia di utilizzo della posta aziendale e di internet.

Tutto ciò premesso,

Mario Aliberti



le Parti convengono che, ai sensi dell'art. 11 bis, comma 4, quinto capoverso, gli accordi condivisi in data odierna e allegati al presente verbale costituiranno un modello di riferimento da utilizzarsi in sede di confronto aziendale per la sottoscrizione degli accordi tra ciascuna BCC/Azienda e le rispettive RR.SS.AA.

Le Parti concordano che restano impregiudicate le specificità di ogni singola Bcc/Azienda e le modulazioni consentite dalle norme che saranno oggetto di definizione in sede aziendale.

ICCREA BANCA S.p.a.

La Delegazione Sindacale di Gruppo

FABI
Mario Al. band.

FIRST-CISL
[Signature]

FISAC-CGIL
[Signature]

UGL CREDITO
[Signature]

UILCA/UIL
[Signature]

VERBALE DI ACCORDO
in materia di videosorveglianza delle filiali ai fini di prevenzione antirapina e tutela del
patrimonio aziendale

Tra

La Banca di Credito Cooperativo di/ La Società, con sede
....., Via, in persona del (di seguito, per brevità, anche indicata come la
"BCC")

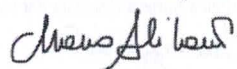
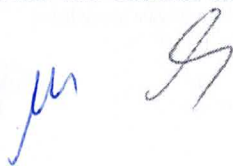
e

Le RR.SS.AA. costituite in:

- FABI
- FIRST-CISL
- FISAC-CGIL
- UILCA
- UGL CREDITO

premesso che

- i. l'intervenuta modifica dell'art. 4 della legge 20 maggio 1970, n. 300, disposta dall'art. 23 del Decreto Legislativo 14 settembre 2015, n. 151, ha introdotto novità di rilievo in tema di "impianti audiovisivi" e "altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori";
- ii. L'art. 4, comma 1, della legge 20 maggio 1970, n. 300 prevede che gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro e dalla tutela del patrimonio aziendale, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati previo accordo sindacale con le Rappresentanze Sindacali Aziendali;
- iii. L'European Data Protection Board ("EDPB") ha emanato, in data 29 gennaio 2020, le Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, che disciplinano le misure di sicurezza organizzative e tecniche da porre in essere nell'ambito dei trattamenti di videosorveglianza;
- iv. Il Gruppo Bancario Cooperativo Iccrea ha recepito le Linee Guida sopra citate attraverso l'emanazione di proprie Linee Guida interne, allegate alla Politica di Gruppo per la Protezione dei Dati, ed ha disciplinato il trattamento effettuato mediante dispositivi di videosorveglianza prevedendo che ciascun titolare del trattamento effettui una valutazione di impatto sulla



protezione dei dati (c.d. DPIA) ed una valutazione della base legale del legittimo interesse (c.d. LIA). Tali presidi sono previsti da ciascuna Società del Gruppo;

- v. In data 25 maggio 2018 è divenuto pienamente applicabile il Regolamento Generale sulla Protezione dei Dati Personali (UE) 2016/679 (anche "GDPR"), recante, a livello europeo, norme uniformi sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.
- vi. Il D.lgs. 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", novellato dal D.lgs. 10 agosto 2018, n. 101, al fine di armonizzare il previgente Codice con la nuova normativa europea in materia di protezione dei dati (GDPR) stabilisce che " il trattamento dei dati personali avviene secondo le norme del Regolamento UE 2016/679 e del Codice stesso, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona";
- viii. La BCC di conferma e ribadisce di non perseguire alcuna specifica finalità diretta e indiretta di controllo a distanza dell'attività dei lavoratori derivante dall'utilizzo dei sistemi di cui al presente Accordo.
- ix. La BCC dichiara altresì di non fare ricorso a strumenti di intelligenza artificiale nell'ambito della videosorveglianza.
- x. In relazione alle fattispecie regolate con il presente Accordo, la BCC di non adotterà nei confronti dei lavoratori interessati provvedimenti disciplinari, salvo i casi di comportamenti che contravvengono a norme di legge o di CCNL, posti in essere con dolo o colpa grave¹.
- xi. Nell'adozione e nell'utilizzo degli impianti/strumenti la BCC di terrà, per quanto ovvio, conto delle normative in materia di sicurezza, prevenzione e protezione sul lavoro (ivi comprese le attribuzioni e i compiti assegnati dal D. Lgs. 81/2008 e successive modifiche e integrazioni ai Rappresentanti dei Lavoratori per la Sicurezza e, ove presenti, alle Rappresentanze Sindacali Aziendali), nonché a quelle relative alla Privacy.
- xii. La sicurezza è un diritto fondamentale per i lavoratori della BCC di;
- xiii. la sicurezza riguarda sia l'integrità della Società nel suo complesso sia l'incolumità delle persone che si trovino all'interno dei locali della Società stessa;
- xiv. l'attività bancaria è notoriamente esposta a rischi di possibili rapine, furti ed altri eventi criminosi, per le sue modalità d'esercizio e la presenza di consistenti giacenze di denaro;
- xv. gli impianti di videosorveglianza e i sistemi antirapina possono essere un valido strumento di prevenzione e deterrenza;

¹ Con la locuzione "colpa grave" si intende la violazione degli obblighi di diligenza causata da un errore palesemente ed inequivocabilmente grossolano e macroscopico, con un evidente comportamento che si discosti dalle basilari regole di diligenza, prudenza e perizia richieste dal caso concreto, ovvero una condotta di straordinaria ed inescusabile imprudenza.

Mario Al.

mu

[Signature]

[Signature]

[Signature]

tutto ciò premesso, le Parti *ut supra* indicate, nel pieno rispetto dell'art. 4 della Legge n. 300/1970 e della vigente disciplina in materia di Privacy (Reg. UE 679/2016, Codice Privacy, Linee guida 3/2019 EDPB sul trattamento dei dati personali attraverso dispositivi video, Provvedimento del Garante della privacy sulla videosorveglianza dell'8 aprile 2010), ad ogni effetto di legge e di regolamento, intendono favorire l'attuazione dei sopra citati Provvedimenti, fermo il relativo ambito di applicazione, in relazione alle previsioni di cui all'art. 4 della legge 20 maggio 1970, n. 300, nel rispetto delle esigenze di tutela individuale, di quelle aziendali, nonché delle specifiche prerogative sindacali e, conseguentemente,

convengono e stipulano quanto segue:

- 1) Le premesse costituiscono parte integrante del presente accordo, che riguarda esclusivamente misure di prevenzione e deterrenza di eventi criminosi.
- 2) L'installazione di un sistema di videosorveglianza a presidio della Sede, delle Filiali, degli uffici di direzione generale e degli ATM è finalizzata a garantire la massima efficacia della funzione di prevenzione e deterrenza di furti, rapine e danneggiamento del patrimonio aziendale, restando esclusa ogni altra possibilità di utilizzo.
- 3) In relazione alle finalità del presente accordo, la Banca installa un impianto di videosorveglianza presso la Sede e presso le Filiali, gli sportelli di tesoreria e gli ATM. La tipologia di impianto, il posizionamento, le modalità di funzionamento e la dislocazione sono indicati nelle planimetrie dei locali, che sono conservate presso la Sede della Banca e sono accessibili da parte delle RR.SS.AA. o delle Autorità competenti, restando esclusa – per evidenti ragioni di sicurezza – la possibilità di estrarne copia. La BCC comunicherà alle RR.SS.AA. ogni eventuale successiva modifica intervenuta nelle planimetrie riguardo alla variazione della tipologia di impianto, le modalità di funzionamento o la dislocazione e posizionamento dell'impianto di videosorveglianza.
- 4) Fermi i profili di sicurezza perseguiti e le finalità sopra indicate, la Bcc /l' Azienda dichiara che l'orientamento delle telecamere è realizzato in modo da limitare al minimo, e comunque in casi residuali rispetto alle finalità perseguite, l'inquadratura di singoli lavoratori.
- 5) Le telecamere non riprendono luoghi il cui accesso è riservato solo ed esclusivamente al personale dipendente (quali ad es. servizi igienici, zona caffè, area fumatori, zona ristoro o mensa).
- 6) Nel caso le immagini possano contenere anche l'inquadratura di postazioni di lavoro, la Banca utilizzerà le registrazioni solo in caso di eventi criminosi, per mettere le stesse a disposizione dell'autorità di polizia e/o dell'autorità giudiziaria dietro specifica richiesta. Resta salvo il diritto del dipendente di richiedere l'accesso alle immagini che lo riguardano. Il trattamento dei dati ha



la durata massima corrispondente a quella di legge per la singola categoria di dati e la specifica finalità, come meglio dettagliato al successivo punto 8).

7) Le Parti concordano che la visualizzazione delle immagini registrate potrà essere effettuata esclusivamente dal personale appositamente incaricato previa compilazione del registro degli accessi che dovrà essere reso disponibile alle OO.SS. a richiesta, secondo la vigente normativa in materia Privacy.

La BCC/Azienda si impegna a comunicare alle OO.SS. i nominativi del personale appositamente incaricato, tempo per tempo, alla visualizzazione delle registrazioni.

Su richiesta del dipendente interessato le immagini visionate saranno rese disponibili, altresì, anche all'Organizzazione Sindacale alla quale conferisce mandato.

Le immagini potranno essere visualizzate in caso di:

- eventi criminosi o atti illeciti che arrechino danno a persone o cose;
- formale richiesta delle FF.OO. o dell'Autorità Giudiziaria;
- richiesta di accesso di un interessato ai sensi dell'art. 15 del GDPR previo opportuno oscuramento di dati di terzi.

8) La visione delle immagini può avvenire:

- in sincronia con la ripresa, anche individualmente, ad opera degli incaricati del trattamento designati per iscritto
- in tempo differito:
 - a) in caso di atti illeciti che coinvolgano dipendenti della BCC, ad opera dell'incaricato del trattamento designato,
 - b) se richiesto dal dipendente interessato, che potrà farsi assistere dal proprio rappresentante sindacale aziendale,
 - c) da parte di appartenenti alle Forze dell'Ordine o dell'autorità giudiziaria che ne facciano formale richiesta.

Le immagini registrate saranno conservate per un periodo di tempo massimo di 7 giorni, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura uffici, e utilizzate esclusivamente per le finalità sopra indicate e conservate nel pieno rispetto della vigente disciplina in materia di Privacy.

Su richiesta dell'autorità giudiziaria e/o di polizia e in relazione esclusivamente alle attività investigative, le immagini registrate potranno essere conservate per un periodo più lungo.

In caso di registrazione, sia analogica sia digitale, le registrazioni sono conservate nel massimo rispetto delle misure di sicurezza ritenute adeguate al rischio. In tal senso la Società ha svolto una valutazione di impatto sulla protezione dei dati personali ai sensi dell'art. 35 del GDPR (c.d. DPIA).

Mario Aliberti

L'accesso ai sistemi di registrazione è consentito al personale tecnico preposto ad interventi di manutenzione e revisione. Detto personale è opportunamente autorizzato a tali attività, anche laddove si trattasse di personale appartenente a società terze.

Ai fini di tutela dei dipendenti, le RSA costituite avranno facoltà di verificare il corretto utilizzo dell'impianto di videosorveglianza.

La visualizzazione delle immagini in caso di necessità di tutela delle persone e del patrimonio aziendale potrà essere effettuata esclusivamente dai dipendenti appositamente individuati dalla Banca alla visualizzazione delle immagini, ove richiesto in presenza delle RSA.

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 su richiesta delle Autorità, o in caso di richiesta di accesso di un dipendente ai sensi dell'art. 15 del GDPR, previo opportuno oscuramento di dati di terzi) ove richiesto in presenza delle RSA, ovvero di un RSA delegato.

9) Le registrazioni non saranno in alcun modo diffuse all'esterno.

10) La Bcc/l'Azienda esclude qualsiasi tracciamento dei dati relativi alla prestazione lavorativa e che dal sistema di videosorveglianza in esame possa derivare qualunque forma di trattamento di dati personali non necessario in rapporto alle finalità che si intendono perseguire con il presente accordo. Più in generale la Bcc/l'Azienda dichiara di adempiere agli obblighi imposti dal Reg. europeo 2016/679 ("GDPR") ed eventuali successive modificazioni, in particolare con riferimento al rispetto dell'obbligo normativo di trasparenza agli interessati, di cui all' art. 4, comma 3 dello Statuto dei Lavoratori ed art. 13 del Regolamento sopra citato. A tal fine, in ottemperanza alla normativa vigente in materia di Privacy sopra richiamata, l'impianto viene segnalato con appositi cartelli informativi (c.d. "informativa breve" o "di primo livello"), che rinviano all'informativa videosorveglianza completa (c.d. "informativa estesa") disponibile su richiesta presso i locali della Banca e sul sito web della medesima.

Per quanto non espressamente disciplinato nel presente accordo, si rinvia alle "Linee Guida di Gruppo su videosorveglianza e videoregistrazione", che recepiscono tutte le novità normative in materia e che formano parte integrante della Politica di Gruppo per la Protezione dei Dati Personali.

Luogo,/...../2023

Banca di Credito Cooperativo di ...

Le RR.SS.AA.

Messa Al'ba

[Signature]

[Signature]

VERBALE DI ACCORDO
in materia di tracciamento delle operazioni bancarie

Tra

La Banca di Credito Cooperativo di, con sede, Via, in persona del (di seguito, per brevità, anche indicata come la "BCC")

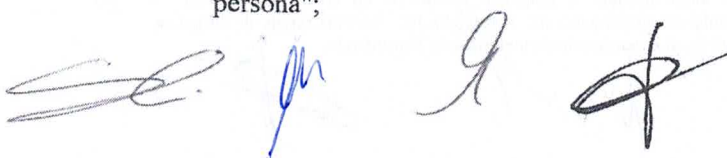
e

Le RR.SS.AA. costituite in:

- FABI
- FIRST-CISL
- FISAC-CGIL
- UILCA
- UGL CREDITO

Premesso che

- i. l'intervenuta modifica dell'art. 4 della legge 20 maggio 1970, n. 300, disposta dall'art. 23 del Decreto Legislativo 14 settembre 2015, n. 151 ha introdotto novità di rilievo in tema di "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"
- ii. Il Garante per la protezione dei dati personali ha emanato, in data 12 maggio 2011, il Provvedimento n. 192 avente ad oggetto "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie", e, in data 18 luglio 2013, il Provvedimento n. 357 che ha differito il termine previsto per l'entrata in vigore al 3 giugno 2014, ulteriormente differita al 30 settembre 2014 dal Provvedimento n. 257 del 22 maggio 2014;
- iii. La BCC ha inteso adeguare i propri sistemi informatici, organizzativi e di processo, alle prescrizioni emanate in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, in applicazione del citato Provvedimento;
- iv. In data 25 maggio 2018 è divenuto pienamente applicabile il Regolamento Generale sulla Protezione dei Dati Personali (UE) 2016/679 (anche "GDPR"), recante, a livello europeo, norme uniformi sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.
- v. Il D.lgs. 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", novellato dal D.lgs. 10 agosto 2018, n. 101 al fine di armonizzare il previgente Codice con la nuova normativa europea in materia di protezione dei dati (GDPR) stabilisce che "il trattamento dei dati personali avviene secondo le norme del Regolamento UE 2016/679 e del Codice stesso, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona";



Maurizio Albi

- vi. La BCC dichiara di non perseguire alcuna specifica finalità diretta e indiretta di controllo a distanza dell'attività dei lavoratori derivante dall'utilizzo dei sistemi di cui al presente Accordo.
- vii. La BCC dichiara altresì di non fare ricorso a strumenti di intelligenza artificiale nell'ambito del tracciamento delle operazioni bancarie.
- viii. In relazione alle fattispecie regolate con il presente Accordo, la BCC non adotterà nei confronti dei lavoratori interessati provvedimenti disciplinari, salvo i casi di dolo e di colpa grave¹.

Considerato che:

- a) Il Provvedimento n. 192/2011 - entrato in vigore il 30 settembre 2014 - è finalizzato a "garantire il rispetto dei principi in materia di protezione dei dati personali ai sensi del D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), in ordine ai temi della 'circolazione' delle informazioni riferite ai clienti in ambito bancario e della 'tracciabilità' delle operazioni bancarie", e detta prescrizioni in relazione al trattamento di tali dati personali della clientela effettuato dai dipendenti delle "banche, incluse quelle facenti parte di gruppi, delle società, anche diverse dalle banche, purché siano parte di tali gruppi", stabiliti sul territorio nazionale;
- b) Il Provvedimento riguarda le operazioni relative ai clienti degli istituti bancari di cui al punto che precede, "sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, cd. inquiry".
- c) Il Provvedimento si applica a tutti i lavoratori "incaricati dall'azienda dei trattamenti" riconducibili nell'ambito di applicazione del Provvedimento n. 192, come chiarito nel successivo Provvedimento n. 357, "quali che siano la qualifica, le competenze, gli ambiti di operatività e le finalità dei trattamenti che sono tenuti a svolgere";
- d) Il Provvedimento, "al fine di assicurare il controllo delle attività svolte sui dati dei clienti e dei potenziali clienti da ciascun incaricato del trattamento", prescrive l'adozione di "idonee soluzioni informatiche" per il controllo dei "trattamenti condotti sui singoli elementi di informazione presenti nei diversi database"; "tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente";
- e) Il Provvedimento, in particolare, stabilisce che "i file di log devono tracciare, per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:
 - a. il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso;
 - b. la data e l'ora di esecuzione;
 - c. il codice della postazione di lavoro utilizzata;
 - d. il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato;

¹ Con la locuzione "colpa grave" si intende la violazione degli obblighi di diligenza causata da un errore palesemente ed inequivocabilmente grossolano e macroscopico, con un evidente comportamento che si discosti dalle basilari regole di diligenza, prudenza e perizia richieste dal caso concreto, ovvero una condotta di straordinaria ed inescusabile imprudenza.

Mario Al. band.

mu

[Signature]

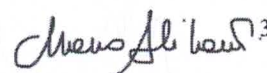
[Signature]

[Signature]

- e. la tipologia del rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata";
- f) Ai sensi del Provvedimento:
- "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, comunque, a personale diverso rispetto a quello cui è affidato il 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, 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" sopra previsto;
 - "l'attività di controllo è 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".
- g) Le misure del Provvedimento debbono essere osservate pure dalle società che operano in outsourcing allorché l'attività esternalizzata sia connessa all'esecuzione di rapporti contrattuali (intercorrenti tra banca e cliente) e richieda l'utilizzo di funzioni applicative a supporto dell'operatività bancaria;
- h) Il Provvedimento n. 192/2011 prescrive che le predette misure siano adottate "nel rispetto della vigente disciplina in materia di controllo a distanza dei lavoratori ex art. 4, comma 1, della Legge 20 maggio 1970, n. 300";
- i) In data 14 maggio 2014 Federcasse e le Segreterie Nazionali delle Organizzazioni sindacali dei lavoratori del Credito Cooperativo hanno sottoscritto un "Accordo quadro" che definisce lo schema generale di accordo da utilizzare per le intese da raggiungere in sede aziendale ex art. 4 della legge 300/1970, in specifica attuazione del Provvedimento sopra citato;
- j) La BCC/Azienda ha illustrato alle RR.SS.AA. e alle Delegazioni Sindacali di Gruppo, nell'incontro odierno, le caratteristiche dei sistemi informatici, dei processi organizzativi e dei processi aziendali, che sono oggetto di adeguamento per garantire la conforme applicazione del Provvedimento n. 192/2011 nel rispetto delle previsioni di cui all'art. 4, comma primo, della legge 300/1970.

Tutto ciò premesso e considerato,

le Parti, nel pieno rispetto dell'art. 4 della Legge n. 300/1970 e della vigente disciplina in materia di Privacy (Reg. UE 679/2016, Codice Privacy, Provvedimento sul tracciamento delle operazioni bancarie 192/2011), ad ogni effetto di legge e di regolamento, intendono favorire l'attuazione dei sopra citati Provvedimenti, fermo il relativo ambito di applicazione, in relazione alle previsioni di cui all'art. 4 della Legge 20 maggio 1970, n. 300, nel rispetto delle esigenze di tutela individuale, di quelle aziendali, nonché delle specifiche prerogative sindacali.



La BCC/Azienda assicura che 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.

Inoltre, si impegna a conservare i log di tracciamento delle operazioni di inquiry per un periodo di 24 mesi dalla data di registrazione dell'operazione, fatte salve esigenze di forza maggiore, con la consapevolezza che oltre tale limite temporale la conservazione è ammessa in presenza di specifici vincoli di legge in materia.

Come espressamente richiesto dal Garante, nell'ambito dei predetti sistemi informativi sono attivati "specifici alert" finalizzati ad individuare "comportamenti anomali o a rischio" relativi alle operazioni di inquiry eseguite dagli incaricati del trattamento. Tali alert saranno individuati dalla BCC/Azienda, ed elencati di seguito, tenendo conto dei range rappresentati nelle Linee Guida di Gruppo (allegato 1 al presente accordo) a riferimento di ciascun parametro.

I parametri in uso sono:

- richieste ripetute con visualizzazione massiva; accesso fuori orario;
 - accesso ripetuto ai dati di un cliente da parte dello stesso operatore;
 - accesso ai dati di un cliente di una filiale diversa dall'operatore;
 - accesso ripetuto ai dati di un cliente da parte dello stesso operatore fuori orario;
 - accesso ai dati di un cliente di una filiale diversa dall'operatore fuori orario;
 - accesso ripetuto ai dati di un cliente di una filiale diversa dall'operatore fuori orario;
 - richieste ripetute con visualizzazione massiva fuori orario;
 - richieste ripetute con visualizzazione massiva sui dati di una filiale diversa;
 - richieste ripetute con visualizzazione massiva sui dati di una filiale diversa fuori orario.
- Per un dettaglio sulle ulteriori specifiche tecniche si rinvia al "Manuale utente Tracciabilità Operazioni_Analisi Log Operazioni di Consultazione" allegato 2.

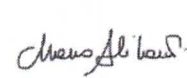
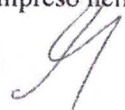
Qualora tali parametri dovessero subire modifiche, la BCC/Azienda tempestivamente lo porterà a conoscenza delle RR.SS.AA e della Delegazione sindacale di Gruppo.

La BCC/L'Azienda dichiara che l'applicativo deputato al tracciamento delle operazioni bancarie rappresenta la soluzione informatica per effettuare la registrazione delle operazioni di consultazione dei dati bancari della clientela in appositi log, conservare in sicurezza detti log per i tempi previsti, consentire il controllo periodico della tenuta degli stessi e le necessarie verifiche sui loro contenuti, nonché fornire un sistema di generazione e gestione di alert. Il trattamento di tali dati è stato oggetto di una valutazione di impatto ex art. 35 del Regolamento (UE) 2016/679 (c.d. GDPR), il cui modello è stato fornito dalla Capogruppo Iccrea Banca Spa, che ha verificato la sussistenza di misure di sicurezza adeguate al trattamento, tali da ricondurre la rischiosità dello stesso ad un livello di rischio accettabile.

La BCC/Azienda assicura che i lavoratori incaricati, sono resi edotti delle procedure adottate e dei connessi adempimenti tramite un'apposita informativa (ex art. 13 del GDPR), fornita attraverso specifici ed opportuni strumenti aziendali.

Inoltre, nell'ambito di quanto previsto dall'art. 63 del CCNL 9.01.2019, come modificato dall'accordo di rinnovo, possono svolgersi, ove necessario, specifiche attività formative retribuite.

La BCC/Azienda garantisce che è escluso qualsiasi utilizzo dei dati tracciati/trattati non espressamente compreso nelle fattispecie normate dal presente verbale di accordo.



Luogo,/...../ 2023

Banca di Credito Cooperativo di ...

Le RR.SS.AA.

.....



Mehmet Ali Kaya

