

## ACCORDO IN MATERIA DI ATTUAZIONE DELL'ART. 4 L. N. 300/1970

In Milano, in data 22 dicembre 2023

tra

- Intesa Sanpaolo S.p.A., anche nella qualità di Capogruppo (di seguito ISP)

e

- le Delegazioni di Gruppo delle OO.SS. FABI, FIRST/CISL, FISAC/CGIL, UILCA e UNISIN

premessi che:

- gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, in considerazione della rilevanza del tema, sono stati nel tempo oggetto di accordi sindacali aziendali nel rispetto delle previsioni normative;
- gli sviluppi tecnologici seguiti all'intervenuta modifica dell'art. 4 della L. n. 300/1970 disposta dal D. Lgs. n. 151/2015 hanno aggiornato gli strumenti e i software utilizzati per rendere la prestazione lavorativa, con aspetti rilevanti in tema di disciplina dei controlli a distanza, rendendo così necessario un nuovo accordo di revisione complessiva della materia al fine di continuare ad assicurare adeguate tutele in relazione alle tecnologie, nel rispetto dei provvedimenti emanati tempo per tempo in materia da parte del Garante della Privacy;
- le novità normative, regolate con l'Accordo 15 marzo 2017 (e successivi aggiornamenti), hanno di fatto introdotto, qualora sia fornita ai dipendenti adeguata informazione in merito alle modalità d'uso degli strumenti e all'effettuazione dei controlli conformemente alle previsioni normative in materia di trattamento dei dati personali, nel rispetto di quanto disposto dal Regolamento UE 2016/679, la possibilità di utilizzo, a tutti i fini connessi al rapporto di lavoro, delle informazioni raccolte nello svolgimento della prestazione lavorativa, non prevedendo la necessità di un accordo sindacale per gli strumenti utilizzati al fine di rendere la prestazione lavorativa, nonché per quelli relativi alla registrazione degli accessi e delle presenze;
- con il citato Decreto Legislativo n. 151/2015 era stata inoltre ridefinita la modalità di coinvolgimento sindacale in materia relativamente agli strumenti/apparecchiature adottati per finalità di organizzazione del lavoro o per difesa del patrimonio aziendale, non rientranti tra gli strumenti strettamente necessari per rendere la prestazione lavorativa, introducendo la possibilità di sottoscrivere Accordi a livello di singola azienda o di Gruppo e ampliando in tal modo il perimetro di applicazione e di validità delle intese anche alle Unità Produttive prive di RSA;
- il vigente Protocollo delle Relazioni Industriali conferma tra le materie di competenza della Delegazione Sindacale di Gruppo anche le previsioni relative agli impianti audiovisivi e agli altri strumenti di controllo, risultando così rispondente alle disposizioni contenute nell'articolo 4 della L. n. 300/1970 come da ultimo modificata;
- le Parti, con la sottoscrizione del presente Accordo, intendono regolare le modalità di utilizzo degli strumenti necessari alla prestazione lavorativa, alla tutela del patrimonio aziendale ed alla

sicurezza. L'Azienda garantisce il pieno rispetto dei principi vigenti in materia di tutela della privacy e, in particolare, il pieno rispetto dei principi applicabili al trattamento dei dati personali, tenuto tra l'altro conto di quanto previsto agli artt. 5 e 35 del Regolamento UE 2016/679 che l'Azienda ha la responsabilità di applicare;

e considerato che:

- il percorso fino ad oggi condiviso con le OO.SS. mediante specifiche intese in materia di tracciatura delle operazioni bancarie e in materia di controlli a distanza (rispettivamente con gli Accordi 12 maggio 2014, 15 marzo 2017 e successivi aggiornamenti) ha permesso di perseguire gli obiettivi di tutela delle esigenze organizzative e produttive, nonché della sicurezza e del patrimonio aziendale;
- alla luce delle evoluzioni tecnologiche si rende ora necessario un nuovo e complessivo accordo al fine di rendere il quadro delle regole applicabili in materia omogeneo e meglio rispondente alla complessità organizzativa e all'articolazione operativa di ciascuna azienda, preservando l'impianto normativo, le logiche contrattuali, le tutele previste per le persone consentendone la sottoscrizione in via esclusiva a livello di Gruppo, anche nel rispetto del Protocollo delle Relazioni Industriali;

si conviene quanto segue:

1. la premessa forma parte integrante e sostanziale del presente Accordo;
2. il presente Accordo da oggi sostituisce le previgenti intese per la specifica regolamentazione in materia di tracciatura delle operazioni bancarie (Provvedimento n. 192 del 12 maggio 2011 del Garante per la protezione dei dati personali) e di controlli a distanza per l'intero ambito nazionale presso le Società del Gruppo Intesa Sanpaolo che applicano il CCNL del credito;
3. fermo quanto previsto in materia da norme di Legge e/o Regolamentari di equivalente valore, nel confermare l'esclusione della finalità del controllo a distanza dell'attività dei lavoratori, le Parti intendono regolare le seguenti materie:
  - A. sistemi di videosorveglianza
  - B. sistemi di registrazione dei canali audio e video
  - C. ulteriori strumenti - sistemi informatici/hardware/software - sistemi di telecomunicazione e di geolocalizzazione - accessi ad aree aziendali
  - D. tracciatura delle operazioni bancarie
  - E. adeguata informazione

#### DICHIARAZIONE DELL'AZIENDA

Nell'ambito di quanto previsto dal presente accordo l'azienda dichiara che darà eventualmente corso a procedimenti disciplinari utilizzando unicamente dati raccolti per le finalità strettamente legate alla normativa di legge e/o Regolamentare di pari valore ed agli scopi di cui in premessa.

### **3.A. SISTEMI DI VIDEOSORVEGLIANZA**

Le Parti confermano che l'ubicazione, l'installazione e l'utilizzo degli impianti di videosorveglianza anche dotati di videoregistrazione sono finalizzati, nel rispetto delle normative tempo per tempo vigenti in materia, 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.

Le caratteristiche tecniche degli impianti, le loro modalità di installazione e di utilizzo nonché quelle di conservazione delle immagini sono allegate al presente Accordo.

I tempi di conservazione delle immagini registrate sono quelli stabiliti dalle normative tempo per tempo vigenti in materia, tenuto conto delle specificità dell'attività bancaria.

In caso di videoregistrazione l'accesso alle immagini registrate sarà possibile solo tramite l'intervento di un limitato numero di dipendenti, specificamente identificati e nominati da parte della società del Gruppo interessata, nonché ove necessario, da tecnici specializzati della ditta manutentrice.

Al fine di consentire a livello decentrato la verifica tecnica dell'attuazione delle intese di Gruppo in caso di attivazione di nuovi impianti, l'Azienda metterà preventivamente a disposizione dei dirigenti delle RR.SS.AA., ovvero, in mancanza degli stessi, ai Coordinatori RR.SS.AA. competenti, la relativa documentazione, comprensiva, in particolare, delle planimetrie e delle schede tecniche descrittive, concernenti l'ubicazione e le caratteristiche degli impianti di videoregistrazione delle singole Unità Organizzative interessate e insistenti nell'Unità Produttiva.

Le OO.SS. indicate potranno quindi provvedere ad un comune sopralluogo di verifica tecnica previa intesa, in merito a data ed ora dello stesso, con i Responsabili delle singole Unità Organizzative, cui compete altresì la custodia della documentazione illustrativa.

Ove dalla verifica tecnica delle OO.SS. emergessero difformità, tali evidenze dovranno essere rappresentate alle competenti funzioni aziendali entro trenta giorni dalla messa a disposizione della documentazione, fatte salve le eccezioni in cui motivate esigenze oggettive richiedano un termine maggiore.

A fronte delle suddette evidenze, qualora le osservazioni pervenute nei termini risultino, a seguito di verifica, tecnicamente fondate, l'Azienda provvederà agli adeguamenti conseguenti (logistici/tecnici/planimetrici) di massima entro trenta giorni e comunque in un arco temporale necessariamente commisurato agli stessi. In caso contrario le OO.SS. potranno richiedere la convocazione di un apposito Comitato di Consultazione, che sarà coinvolto con le modalità previste in allegato, al fine di dirimere la problematica insorta adottando le conseguenti determinazioni. Ove sia stato esperito inutilmente tale processo, in coerenza con quanto stabilito dall'articolo 3 del vigente Protocollo delle Relazioni Industriali, resta confermata la possibilità di agire nell'ambito delle prerogative di ciascuna delle Parti.

Accertata la rispondenza delle informazioni rappresentate ovvero al termine del processo descritto, la documentazione tecnica si intenderà consolidata fino alla successiva eventuale revisione/modifica.

In relazione agli eventuali interventi di modifica e sostituzione delle apparecchiature, sarà adottata la medesima procedura sopra descritta, ferma restando la necessaria rispondenza degli impianti ai principi del presente Verbale.

### **3.B. SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO E VIDEO**

Presso il Gruppo Intesa Sanpaolo, in ragione delle differenti caratteristiche delle attività lavorative interessate, le registrazioni dei canali audio e video degli strumenti utilizzati per rendere la prestazione lavorativa, nel rispetto di quanto già previsto in premessa, possono avvenire con le seguenti modalità:

- registrazione parziale su iniziativa del lavoratore solo per la parte strettamente necessaria a ricostruire la fase inerente allo svolgimento della prestazione lavorativa (a titolo esemplificativo: registrazione delle transazioni commerciali di Filiale). Le registrazioni vengono archiviate in via accentrata in locali appositamente allestiti e dotati di sistemi di sicurezza per l'accesso ("server farm") ovvero in apposita soluzione Cloud;

- registrazione integrale in entrata e/o in uscita sugli strumenti facenti capo a ciascun operatore assegnati per lo svolgimento della prestazione lavorativa in azienda o a distanza (a titolo esemplificativo: registrazione delle transazioni commerciali nella Filiale Digitale). Le registrazioni vengono archiviate nelle "server farm" dipartimentali ovvero in apposita soluzione Cloud ad accesso controllato e limitato. In azienda, anche tramite diversi strumenti di work collaboration, gli operatori avranno a disposizione altri canali di comunicazione, non sottoposti a registrazione, per conversazioni personali diverse da quelle relative alle attività lavorative che dovranno godere della dovuta riservatezza. Gli operatori saranno debitamente informati in merito agli strumenti disponibili con indicazione di quelli non soggetti a registrazione e/o di quelli che, pur non essendo soggetti a registrazione, per esigenze di sicurezza e di tutela del patrimonio aziendale prevedono l'acquisizione dei soli metadati.

Le apparecchiature e/o i software di registrazione (telefonia fissa, mobile, strumenti di work collaboration ed equivalenti), che rispondono ai criteri previsti dalla normativa tempo per tempo vigente, sono attivati per l'espletamento di una determinata attività nel rispetto di standard adeguati, in grado di tutelare le esigenze di sicurezza e privacy dei lavoratori. I relativi supporti digitali datati, numerati (ovvero i file archiviati in soluzioni Cloud) sono conservati in base alla normativa tempo per tempo vigente in materia, tenuto conto delle specificità dell'attività bancaria, e custoditi con idonea protezione (come specificato in allegato).

Il riascolto delle conversazioni e/o l'accesso alle immagini acquisite avverrà tramite l'impiego di codici/password individuali (ovvero altre modalità di verifica dell'accesso di pari tutela), nei casi di seguito specificati:

- riascolto/accesso ad iniziativa individuale: nel caso in cui il sistema consenta il riascolto/l'accesso individuale ed in piena autonomia da parte di ciascun operatore, questi potrà accedere solo alle proprie registrazioni secondo le funzionalità del sistema, con l'immissione di un proprio codice/password identificativo personale;
- riascolto/accesso ad iniziativa dell'Azienda in tutti i casi di richiesta o di contestazione su una transazione ad opera di clienti e/o controparti: il riascolto/l'accesso dovrà avvenire con la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo. Il riascolto/l'accesso potrà svolgersi eventualmente anche mediante collegamento "da remoto" dei soggetti interessati in presenza delle condizioni tecniche necessarie;
- riascolto/l'accesso ad iniziativa dell'Azienda per l'assolvimento delle funzioni di controllo interno previste da norme di legge e/o regolamentari e/o da richieste degli Organi di Vigilanza italiani, europei, extra europei a garanzia della tutela della clientela e/o del patrimonio aziendale.

Tutte le risorse coinvolte nei processi di riascolto, e/o di accesso alle immagini hanno l'obbligo di non registrare né diffondere le informazioni ottenute, garantendo la massima riservatezza.

Nuove esigenze in materia (ad esempio nuove attivazioni della componente video anche lato lavoratore) formeranno oggetto di uno specifico incontro illustrativo con il Comitato di Consultazione, che sarà coinvolto con le modalità previste in allegato per dirimere eventuali controversie relative all'installazione.

### **3.C. ULTERIORI STRUMENTI - SISTEMI INFORMATICI/HARDWARE/SOFTWARE - SISTEMI DI TELECOMUNICAZIONE E DI GEOLOCALIZZAZIONE - ACCESSI AD AREE AZIENDALI**

Ferma restando l'esclusione della finalità del controllo a distanza dell'attività dei lavoratori, in merito agli strumenti utilizzati per rendere la prestazione lavorativa le Parti, attesa la continua evoluzione delle tecnologie - e quindi a titolo non esaustivo - concordano nel definire i seguenti principi relativi a:

- **SISTEMI INFORMATICI: HARDWARE E SOFTWARE**

I diversi sistemi informatici che comportano il ricorso a procedure di identificazione, verbalizzazione/trascrizione, archiviazione (ad esempio di chat e/o e-mail) e/o di abilitazione e consentono l'individuazione dell'operatore che abbia effettuato le singole operazioni e transazioni, e/o di altri elementi come la data di inizio/fine della comunicazione, il fuso orario, l'identificativo dei partecipanti, fermo restando il rispetto di quanto previsto dalla normativa nazionale ed europea di riferimento e, in particolare, dall'art. 4 L.300/1970 (anche in tema di adeguata informazione), sono finalizzati rispettivamente all'esercizio delle attività assegnate, alla sicurezza delle comunicazioni e/o alla tutela del patrimonio aziendale.

Rientrano in questa fattispecie anche gli eventuali software aggiuntivi rispetto a quelli propri dello strumento di lavoro, che permettono di ricostruire le fasi in cui si articolano le transazioni secondo quanto stabilito dalla Direttiva 2004/39/CE del Parlamento europeo e del Consiglio del 21 aprile 2004 relativa ai mercati degli strumenti finanziari (MIFID II, ad oggi art. 76 del Regolamento Delegato UE 2017/565 del 25 aprile 2016, artt. 94 e 95 del Regolamento Intermediari adottato dalla Consob con delibera n. 20307 del 15 febbraio 2018 e successive modifiche), e tenuto conto di quanto previsto dal Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA, ad oggi Code of Federal Regulations - Title 17 - Commodity and Securities Exchanges -, § 1.31, § 23.202 e § 23.602) nonché i sistemi informatici che presidiano la sicurezza degli strumenti di lavoro tutelandone il loro corretto utilizzo quali Data Loss Prevention (DLP), in grado di prevenire i rischi legati alla perdita di dati informatici, o che ricorrono ad ambienti Big Financial Data (BFD) per la tracciatura delle operazioni bancarie.

- **SISTEMI DI TELECOMUNICAZIONE E DI GEOLOCALIZZAZIONE**

Con riferimento agli impianti di telecomunicazione messi a disposizione dall'Azienda (a titolo esemplificativo si indicano le tecnologie che consentono la trasmissione di dati quali i supporti SIM/UMTS/HSDPA), nonché gli strumenti dotati di dispositivi che consentono la geolocalizzazione sulla base delle impostazioni del produttore – inclusa l'eventuale disattivabilità - e senza personalizzazione da parte di ISP, si precisa che la rilevazione dati dei medesimi è utilizzata esclusivamente a fini statistici, di documentazione dei costi e dei dati di traffico/utilizzo, nonché di sicurezza e tutela del patrimonio aziendale.

- **ACCESSI AD AREE AZIENDALI**

Per finalità di sicurezza, tutela del personale e del patrimonio aziendale, l'Azienda continuerà ad utilizzare tutte le tecnologie, a titolo esemplificativo "tornelli" e bussole", per la prevenzione di atti criminosi e per disporre di strumenti idonei a verificare e/o registrare la presenza di persone all'interno di tutti i siti nel rispetto delle norme tempo per tempo vigenti in materia. L'accesso a tali zone potrà avvenire mediante l'utilizzo di badge o altro strumento utile anche ai fini della registrazione dei dati di ingresso e uscita.

L'Azienda può individuare c.d. "aree protette" presso alcuni palazzi, diverse e aggiuntive rispetto a quelle riservate all'ingresso e all'uscita del personale (a titolo esemplificativo: centri elaborazione dati ovvero zone che, per la presenza di particolari dati o persone, sono definite "sensibili"), con controllo degli accessi dedicato e riservato unicamente al personale abilitato.

Tali sistemi di rilevazione provvedono alla concentrazione, alla gestione dei dati rilevati e alla loro archiviazione mediante apposite apparecchiature.

L'accesso ai dati predetti è consentito solo alle funzioni aziendali competenti esclusivamente a fini statistici relativi a rilievi tecnici sui flussi che interessano i singoli apprestamenti del controllo accessi, ovvero ai fini di presa visione dei dati relativi agli accessi alle aree protette nei seguenti particolari ed individuati casi:

- interventi a garanzia della tutela del patrimonio;
- fattispecie che riguardino la sicurezza degli impianti e/o il regolare funzionamento dei medesimi;
- specifiche ed individuate esigenze di verificare la presenza di Personale presso le Aree protette ubicate nei complessi immobiliari dell'Azienda proprie dei Responsabili incaricati dell'esecuzione dei piani di evacuazione, al fine di poter ottemperare puntualmente a quanto stabilito in materia dal D. Lgs. 9 aprile 2008, n. 81 e successive modifiche ed integrazioni.

L'Azienda informerà preventivamente le competenti OO.SS. in sede di Comitato di Consultazione circa l'installazione di nuovi sistemi di controllo accessi, al fine di permettere la verifica del rispetto dei principi sopra enunciati.

Per tutti gli strumenti viene altresì consentito l'effettivo esercizio della funzione di audit/ controllo interno prevista da norme di legge e regolamentari da parte delle strutture aziendali a ciò dedicate, nonché il puntuale assolvimento della tutela del patrimonio aziendale, delle richieste degli Organi di Vigilanza italiani, europei e/o extra europei e indagini dell'Autorità Giudiziaria e/o iniziative delle Autorità di Pubblica Sicurezza, in coerenza con i principi enunciati nel presente Accordo.

Le informazioni raccolte saranno comunque trattate nel rispetto della normativa applicabile in materia di privacy, ivi compreso il Regolamento (UE) 2016/679.

In relazione a tutto quanto precede, Intesa Sanpaolo anche in qualità di Capogruppo, dichiara la propria disponibilità a convocare specifici incontri, anche su richiesta delle OO.SS. firmatarie del presente accordo, nell'ambito del Comitato di Consultazione per analizzare le eventuali sopravvenute esigenze in materia, con particolare attenzione in merito ai nuovi apprestamenti tecnologici che dovranno necessariamente rispondere ai principi contenuti nel presente Accordo. In tale occasione le OO.SS. firmatarie saranno altresì aggiornate sullo stato applicativo delle presenti intese.

### **3.D. TRACCIATURA DELLE OPERAZIONI BANCARIE**

Tenuto conto degli sviluppi normativi e tecnici che nel tempo si sono verificati, il presente documento riprende e aggiorna le intese vigenti in materia nel Gruppo ISP. Secondo quanto rappresentato all'art. 2 del Protocollo Relazioni Industriali 14 aprile 2021, le Parti confermano l'impostazione sin qui adottata per regolare il tracciamento delle operazioni bancarie in tutte le Società del Gruppo ISP destinatarie del CCNL del Credito tempo per tempo vigente e rientranti nell'ambito di applicazione definito dal Provvedimento n. 192 del 12 maggio 2011 del Garante per la protezione dei dati personali.

In particolare:

- le soluzioni informatiche adottate, sono idonee al controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database e sui diversi ambienti Big Financial Data (BFD), anche ai sensi di quanto prescritto dal Garante per la protezione dei dati personali con il Provvedimento n. 192 del 12 maggio 2011.

- 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 autorizzati al trattamento.

I *file* di *log* tratteranno per ogni operazione di accesso ai dati bancari effettuata da un autorizzato, le seguenti informazioni:

- il codice identificativo del soggetto autorizzato che ha posto in essere l'operazione di accesso;
- la data e l'ora di esecuzione;
- il codice della postazione di lavoro utilizzata;
- il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato;
- la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata, unitamente alle eventuali ulteriori informazioni indicate nello specifico allegato del presente Accordo.

Nel caso in cui si evidenziasse la necessità di tracciare ulteriori informazioni rispetto a quelle qui elencate e contenute nell'allegato, le integrazioni saranno oggetto di informativa ed analisi a livello di Comitato di Consultazione con l'eventuale coinvolgimento delle Delegazioni di Gruppo ai sensi e per gli effetti del Protocollo Relazioni Industriali 14 aprile 2021.

- I *log* di tracciamento delle operazioni di *inquiry* saranno conservati per un periodo di 24 mesi dalla data di registrazione dell'operazione, fatte salve esigenze di forza maggiore. Oltre tale limite temporale la conservazione è ammessa in presenza di specifici vincoli di legge in materia.
- Le specifiche tecniche, riportate in allegato, formano parte integrante del presente accordo. Le eventuali future modifiche saranno sottoposte, come detto, al Comitato di Consultazione e costituiranno anch'esse parte integrante del presente accordo.
- Come espressamente richiesto dal Garante, sono attivati specifici *alert* finalizzati ad individuare comportamenti anomali o a rischio relativi alle operazioni di *inquiry* eseguite dagli autorizzati al trattamento.
- Ai sensi del Provvedimento n. 192 del 12 maggio 2011 e successive integrazioni:
  - 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.
- I lavoratori interessati alla tracciatura ("autorizzati al trattamento") sono informati delle procedure adottate e dei connessi adempimenti tramite apposita informativa, che sarà portata a conoscenza di tutti i lavoratori attraverso specifici ed opportuni strumenti. Inoltre, nell'ambito di quanto previsto in materia di formazione dal CCNL del Credito tempo per tempo vigente, potranno essere previste, ove necessario, specifiche attività formative retribuite.

- In sede aziendale saranno effettuati, a richiesta, incontri di verifica annuale in merito all'applicazione degli accordi in materia con riferimento al numero di *alert* generati.
- Il Comitato di Consultazione è informato in ordine alla/e unità organizzativa/e cui è tempo per tempo affidato il trattamento dei dati bancari dei clienti in base a quanto previsto dal Provvedimento di cui trattasi, nonché sulle modalità di indagine a campione.
- Per quanto altro non espressamente richiamato, si fa rinvio alle prescrizioni del citato Provvedimento del Garante per la protezione dei dati personali della clientela.

### **3.E. ADEGUATA INFORMAZIONE**

Fermo restando che l'Azienda ha l'obbligo di fornire "al lavoratore adeguata informazione delle modalità d'uso degli strumenti" di cui al presente Accordo "e di effettuazione dei controlli", in conformità al Regolamento (UE) 2016/679 e ai provvedimenti emanati tempo per tempo in materia da parte del Garante della Privacy, in assenza della quale i dati non possono essere utilizzati, le specifiche riguardanti tali strumenti lavorativi saranno comunicate anche alle OO.SS. nell'ambito del Comitato di Consultazione, previsto dal vigente Protocollo delle Relazioni Industriali, che sarà altresì convocato per monitorare l'applicazione del presente accordo.

L'Azienda si rende inoltre sin d'ora disponibile a raccogliere in tale sede eventuali evidenze circa gli aspetti applicativi del presente accordo, al fine di valutare le possibili azioni da mettere in atto in coerenza con le intese raggiunte sull'argomento.

#### **DICHIARAZIONE DELL'AZIENDA**

L'Azienda per l'attuazione dell'adeguata informazione prevista dall'art. 4 L. 300/1970 ricorre ad un puntuale aggiornamento delle policy, anche alla luce delle eventuali novità normative, e utilizza i canali informativi ordinariamente riservati alle evidenze di maggiore rilievo per comunicare in modo tempestivo con tutto il personale e per rendere le informative di Legge. Ogni risorsa tramite la Intranet può conoscere la documentazione in materia di controlli a distanza, le relative regole e policy aziendali nonché, tramite il portale #People, le adeguate informative – con sottoscrizione per presa visione - relative alla propria prestazione lavorativa, e fruire dei contenuti formativi necessari per mantenere aggiornate le proprie competenze in materia.

\* \* \*

I principi condivisi nel presente accordo si applicano nel Gruppo ISP a tutti gli strumenti, ivi compresi gli strumenti di lavoro, e saranno applicati anche nel caso si rendesse necessaria l'implementazione e/o l'attivazione di nuovi strumenti: in tal caso si procederà comunque all'approfondimento ed analisi in sede di Comitato di Consultazione con il coinvolgimento delle Delegazioni di Gruppo ai fini dell'eventuale adeguamento dell'Accordo e/o della documentazione allegata.

Intesa Sanpaolo (anche in qualità di Banca Capogruppo) e le Delegazioni di Gruppo valuteranno le previsioni del presente Accordo sulla base delle eventuali soluzioni che dovessero essere condivise a livello nazionale in applicazione dell'art. 28 del CCNL 19 dicembre 2019 "Impegni delle Parti - Controlli a distanza".

Di seguito sono allegati a titolo esemplificativo i seguenti documenti che formano parte integrante del presente accordo:

- *Documento descrittivo* (che in base alla tipologia dello strumento ne rappresenta in modo sintetico le caratteristiche);
- *Planimetria - tipo* degli ambienti soggetti a Videosorveglianza;
- *Scheda tecnica* che riepiloga il dettaglio degli strumenti per tipologia e ubicazione.



In base alla tipologia dello strumento, la precedente documentazione può essere integrata da una *Scheda esplicativa*. Nel caso della Videosorveglianza la Scheda esplicativa riportata in allegato è comune a tutti gli impianti, esplicita i criteri seguiti nell'installazione e nel posizionamento delle telecamere aggiungendosi alla documentazione che sarà prodotta, custodita e consultabile a livello locale.

Quanto rappresentato negli allegati esemplificativi è un "percorso guidato" che, in base alla tipologia dello strumento, le funzioni tecniche dovranno seguire per descriverne le caratteristiche.

Di seguito, oltre alla documentazione esemplificativa, a fini ricognitivi si riportano le schede relative alla situazione esistente nel Gruppo, redatte secondo lo schema rappresentato, tenuto conto che alcune strutture possono avvalersi delle medesime tecnologie.

Oltre ai momenti di confronto già previsti nel presente accordo, le Parti si incontreranno di massima annualmente per un aggiornamento in materia.

INTESA SANPAOLO S.p.A.  
(anche n.q. di Capogruppo)

FABI

FIRST/CISL

FISAC/CGIL

UILCA

UNISIN

*Accordo firmato digitalmente*

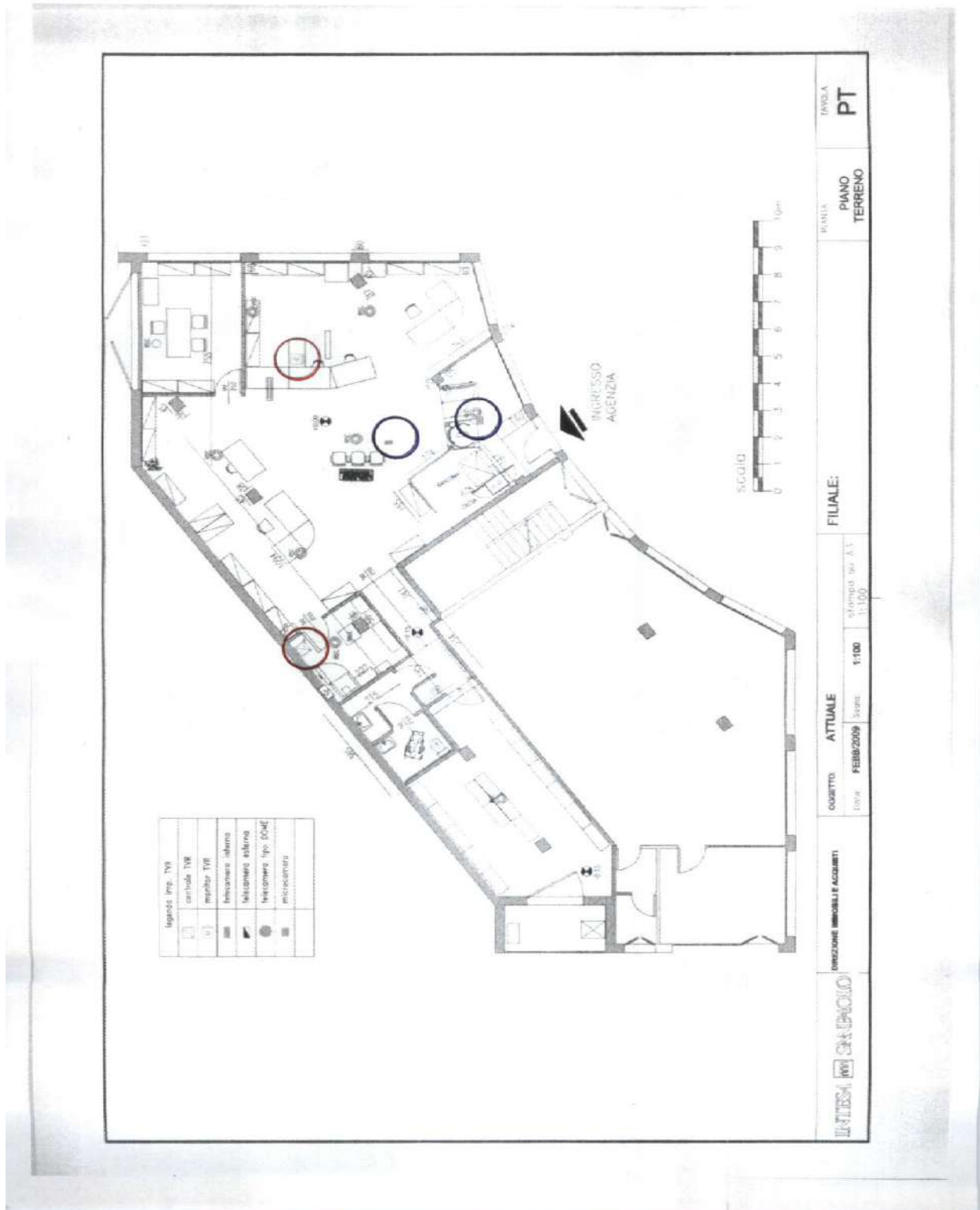
VIDEOREGISTRAZIONE E VIDEOSORVEGLIANZA

(ESEMPIO - DOCUMENTO DESCRITTIVO)

U. P. di ...

Tipo Impianto	Videoregistrazione
Videosorveglianza	Videosorveglianza remota degli ambienti da parte di personale specializzato (es. Global Security System/Control Room)
Caratteristiche tecniche Videoregistrazione	Sistema DIGITALE che registra 24 ore al giorno durante tutto l'anno inclusi i sabati e le domeniche su idoneo supporto (ad oggi hard disk).  Sistema ANALOGICO che registra dal lunedì al venerdì su supporto magnetico.
Ubicazione	Armadio protetto da chiave
Supporti	Sistema DIGITALE: la registrazione delle immagini viene effettuata su hard disk.  Sistema ANALOGICO: la registrazione delle immagini avviene su videocassetta/VHS.
Termini di conservazione	Conforme a quanto previsto tempo per tempo dalla vigente normativa in materia (ad oggi 7gg.). L'accesso ai dati videoregistrati non è consentito al di fuori dei casi previsti dalla normativa di legge.
Modalità	Sistema DIGITALE: hard disk, in locali protetti e ad accesso controllato o all'interno di armadi di sicurezza, con eventuale password/chiave elettronica in capo ai soggetti normativamente indicati.  Sistema ANALOGICO: videocassetta in locali protetti e ad accesso controllato o all'interno di armadi di sicurezza con custodia chiavi secondo le indicazioni normative tempo per tempo vigenti.

ESEMPIO - PLANIMETRIA



## **Scheda esplicativa**

### **(criteri comuni a tutti gli impianti di Videosorveglianza soggetti a registrazione)**

#### **A. TIPOLOGIA SISTEMI DI VIDEOREGISTRAZIONE**

I sistemi di videoregistrazione possono essere di due tipi: in via principale sistema digitale con registrazione su idoneo supporto (ad oggi hard disk) 24h al giorno per tutto l'anno – inclusi sabato e domenica – ovvero, in via residuale, sistema analogico con registrazione dal lunedì al venerdì su supporto magnetico. Tutte le registrazioni sono archiviate in locali protetti e ad accesso controllato o all'interno di armadi di sicurezza protetti.

#### **B. CRITERI RELATIVI ALLA SELEZIONE DEI PUNTI DI RIPRESA**

I criteri di selezione delle aree riprese attraverso gli impianti di videoregistrazione e TV.CC, qualora non vi siano allestite postazioni fisse di lavoro, sono:

- a. perimetro dei locali di pertinenza della Banca/Società. Sono inclusi i varchi perimetrali quali punti di possibili intrusioni non autorizzate (porte perimetrali, finestre, intercapedini, ecc.).
- b. atrio e/o zona pubblico e/o area di ingresso principale/secondario ai locali;
- c. aree "critiche" o ad alta sicurezza, ove sono ubicati gli "asset" più importanti (valori/informazioni/infrastrutture) da proteggere. Sono inclusi caveau, mezziforti, aree self banking, locali server/apparati di telecomunicazioni, locali macchine, o altri ambienti oggetto di intrusioni ai fini di sabotaggio;
- d. filtri di transito, per la selezione delle persone autorizzate al passaggio, interni ed esterni, quali bussole, porte interbloccate, tornelli.

#### **C. TUTELA DELLA PRIVACY**

I tempi di conservazione delle immagini sono quelli stabiliti dalle normative tempo per tempo vigenti in materia, con specifico riferimento all'attività bancaria, attualmente pari a sette giorni.

L'accesso ai dati videoregistrati non è consentito al di fuori dei casi previsti dalla normativa di legge:

- richiesta formale delle Forze di Polizia e/o dell'Autorità Giudiziaria;
- istanza da parte del soggetto interessato al trattamento dei dati personali.

L'eventuale acquisizione di immagini da parte delle Forze di Polizia e/o dell'Autorità Giudiziaria deve avvenire contro rilascio di verbale di sequestro o di acquisizione.

Il pubblico che accede all'unità operativa della Banca in cui è attiva la videoregistrazione viene informato secondo le modalità previste dalla normativa tempo per tempo vigente in materia.

Il Direttore della Filiale (o un dipendente specificatamente individuato per un Palazzo di sede Centrale/Società), è autorizzato al trattamento dei dati personali ed a questi è normativamente attribuita, tra altre previsioni, la gestione delle chiavi dei locali protetti e/o dell'armadio di sicurezza che contiene il videoregistratore e la corretta conservazione di eventuali password per l'accesso ai dati.

SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO/VIDEO

(ESEMPIO - DOCUMENTO DESCRITTIVO)

U. P. di ...

Tipo Impianto	Apparecchiature / canali audio/video in dotazione
Caratteristiche tecniche	Sistema DIGITALE
Ubicazione	Apprestamenti periferici siti in Filiali per la registrazione degli ordini, con archiviazione presso appositi storage dotati di sistemi di protezione e backup localizzati in Server Farm
Supporti	Hard Disk presso Server Farm
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di riascolto	La ricerca della registrazione avviene previo inserimento, secondo procedura, dei parametri identificativi richiesti. L'accesso è consentito attraverso chiavi digitali.

ESEMPIO - SCHEDA TECNICA

Scheda tecnica

DATI FILIALE		VIDEOREGISTRAZIONE					REGISTRAZIONI DEGLI ORDINI TELEFONICI		
PR.	COMUNE	INDIRIZZO	CAP	VIDEOSORVEGLIANZA	CARATTERISTICHE TECNICHE	N° TELECAMERE	N° MONITOR	SUPPORTI	PLANIMETRIE
XX	Filiale 1	esempio 1	1000	NO	Analogico 2	1	1	VHS	3
XX	Filiale 2	esempio 2	1000	SI	Digitale 7	1	1	Hard-Disk	1
								Server Farm	Server Farm
								Digitale	Digitale
								Digitale	Digitale

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

Intesa Sanpaolo:  
FILIALE DIGITALE, FILIALE DIGITALE SPECIALIZZATA, FILIALI REMOTE, PULSE, ISYBANK,  
SERVICE FDI FIDEURAM INTESA SANPAOLO PRIVATE BANKING  
Assistenza Rete e Clienti, Banca Diretta - Contact Center, Active Clients Trading e Servizi di Trading  
(Execution Desk di Trading Evoluto)

DOCUMENTO DESCRITTIVO  
(tecnologia comune a tutte le sedi e ai distaccamenti aziendali  
delle strutture richiamate)

Tipo impianto	Cisco - A.S.C. – PowerPLay
Caratteristiche tecniche	<i>Apparati di registrazione ASC Marathon Evoip v.10</i> su server virtuali Windows attestati in server farm dipartimentali.
Ubicazione	Impianti custoditi presso server farm dipartimentali
Supporti di registrazione	Registrazione su disco di Virtual Machine replicato su più server farm e archiviazione su N.A.S.
Termine di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di registrazione e riascolto.	<p>La soluzione di registrazione archivia le telefonate su una componente di prodotto chiamata I.A.S. La soluzione tecnica su cui sono installati tali componenti è basata su Virtual Machine Windows situate nelle server farm dipartimentali e sfruttano le componenti di archiviazione protetta degli storage. Tutte le registrazioni sono criptate, ricercabili e accessibili su piattaforma Evoip v10 mediante un componente web previsto dalla soluzione.</p> <p>L'accesso alle registrazioni avviene mediante una abilitazione temporanea che la funzione preposta rende visibile per 15 minuti all'addetto incaricato di rendere disponibili per il riascolto la/le telefonata/e.</p> <p><b>RIASCOLTO DA REMOTO O PRESSO LE SEDI AZIENDALI:</b> Mediante accesso profilato per la ricerca della conversazione, la funzione preposta abilita l'addetto a individuare la telefonata sul server e a operare in una sessione di condivisione che dovrà essere da lui inoltrata a tutti i partecipanti alla procedura. L'addetto al riascolto si collega allo spazio di collaborazione al quale sono collegati i partecipanti del riascolto e, individuata la telefonata, ne attiva la riproduzione, provvedendo a condividere il proprio schermo comprensivo di audio.</p>

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

Intesa Sanpaolo:

FILIALE DIGITALE, FILIALI REMOTE, PULSE, ISYBANK,  
SERVICE FDI FIDEURAM INTESA SANPAOLO PRIVATE BANKING

Assistenza Rete e Clienti, Banca Diretta - Contact Center, Active Clients Trading e Servizi di Trading  
(Execution Desk di Trading Evoluto)

### DOCUMENTO DESCRITTIVO

(tecnologia comune a tutte le sedi aziendali e ai distaccamenti  
delle strutture richiamate)

<p>Modalità di registrazione e riascolto (segue).</p>	<p>Al termine del processo, l'addetto al riascolto salva il file audio riascoltato in una share profilata e redige, ove necessario, un verbale di trascrizione della conversazione riascoltata.</p> <p>Ogni generazione della chiave temporanea ed il conseguente accesso saranno censiti in un apposito registro informatico visionabile su richiesta scritta da parte delle RR.SS.AA. abilitate al riascolto ovvero da parte delle Segreterie degli Organi di Coordinamento delle medesime sigle.</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p> <p>L'infrastruttura descritta in precedenza ospita anche la registrazione delle interazioni tra la componente di intelligenza artificiale presente sul risponditore automatico di Filiale Digitale (da ora "Ellis") ed i clienti. Tutte le registrazioni delle interazioni di Ellis sono distinguibili puntualmente rispetto a quelle dei gestori di Filiale Digitale mediante l'aggiunta di informazioni di tracciatura dedicate che permettono sia l'identificazione puntuale che una segregazione applicativa rispetto a quelle dei gestori. L'accesso alle registrazioni di Ellis, oltre a fini di controllo, può essere eseguito dal personale di Filiale Digitale per migliorare il modello di comprensione della componente di intelligenza artificiale.</p>
---	---



## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO VIDEOBANKING

Intesa Sanpaolo:  
FILIALI DIGITALI REMOTE

DOCUMENTO DESCRITTIVO  
(tecnologia comune a tutte le sedi aziendali delle strutture richiamate)

Tipo impianto	Cisco Webex – Theta Lake – Portale Web Theta Lake
Caratteristiche tecniche	Theta Lake soluzione SaaS
Ubicazione	Cloud Theta Lake in UE
Supporti di registrazione	NAS su cloud Theta Lake in UE
Termine di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di registrazione e riascolto.	<p>La soluzione di registrazione archivia la traccia audio delle Videochiamate eseguite mediante la soluzione di collaboration Cisco Webex tramite una soluzione cloud, sempre di tipo SaaS, il cui fornitore è Theta Lake.</p> <p>La soluzione Theta Lake permette l'archiviazione delle registrazioni, secondo quanto previsto dalla normativa vigente, in modalità protetta e fornisce la possibilità di ricercare puntualmente ogni contatto.</p> <p>In caso di necessità, il riascolto avviene mediante la FDI che si mette in contatto con la struttura GT che ha in gestione la piattaforma Cloud. Questa si occupa di effettuare la ricerca del file audio e di depositarlo su un repository posizionato su infrastruttura Banca il cui accesso è limitato al richiedente e alla funzione IT.</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO

ARCHIVIO STORICO BANCA 5

DOCUMENTO DESCRITTIVO

Tipo impianto	Redbox
Caratteristiche tecniche	Prodotto: Redbox Quantify Versione: 6C SP1
Ubicazione	Impianti custoditi presso server farm dipartimentali
Supporti di registrazione	Archiviazione dei dati su NAS
Termine di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di registrazione e riascolto.	<p>FDI In caso di necessità, il riascolto avviene mediante la FDI (secondo le modalità descritte nel relativo allegato). A questo scopo la struttura GT responsabile delle componenti tecnologiche mette a disposizione della FDI il file audio criptato della conversazione oggetto di riascolto.</p> <p>Ogni invio alla FDI dei suddetti file unitamente alla conferma dell'avvenuto riascolto saranno censiti in un apposito registro informatico. Tale registro è visionabile su richiesta scritta da parte delle RR.SS.AA. abilitate al riascolto ovvero da parte delle Segreterie degli Organi di Coordinamento delle medesime sigle.</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

**Scheda Tecnica FDI (e relativi distaccamenti), FDIS, Filiali Digitali Remote collocate in sedi FDI (\*\*)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE FDI</b>	<b>CAP</b>	<b>CARATTERISTICHE TECNICHE</b>	<b>SUPPORTI</b>
MI	Milano (**)	Via Giambellino, 135	20100	Digitale	Server Farm
TO	Moncalieri (**)	Corso Savona, 58	10024	Digitale	Server Farm
NA	Napoli (**)	Via Galeota 31/33	80125	Digitale	Server Farm
BO	Bologna	Via Cairolì 9	40121	Digitale	Server Farm
CA	Cagliari	Viale Bonaria C/O BCS	9125	Digitale	Server Farm
LE	Cavallino (**)	Via Zona PIP Lotto B, 3	73020	Digitale	Server Farm
TP	Trapani	Via Libica, 11	91100	Digitale	Server Farm
PD	Padova (**)	Via Trieste, 57/59	35121	Digitale	Server Farm
RM	Roma	Via Lamaro, 25/a	00173	Digitale	Server Farm
FI	Firenze (**)	Via Carlo Magno, 7	50127	Digitale	Server Farm
TV	Montebelluna (**)	Via Feltrina sud, 250	31044	Digitale	Server Farm
VI	Vicenza (**)	Via Battaglione Framarin, 20	36100	Digitale	Server Farm
PA	Palermo (**)	Via Cusmano, 56	90141	Digitale	Server Farm
PR	Parma (**)	Via Langhirano, 1 PAL B	43100	Digitale	Server Farm
PO	Prato (**)	Via Degli Alberti, 2	59100	Digitale	Server Farm
BB	Bari (**)	Via Abate Gimma, 99	70122	Digitale	Server Farm
CH	Chieti	Via Colonna, 24	66100	Digitale	Server Farm
JE	Jesi	Via Don Angelo Battistoni, 4	60035	Digitale	Server Farm
PU	Pesaro Urbino	Via Gargarin, 216	61122	Digitale	Server Farm
CS	Rende	Via Volta, 92	97036	Digitale	Server Farm

**Scheda Tecnica: Filiali Digitali Remote non collocate presso sedi FDI****REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE TECNICHE</b>	<b>SUPPORTI</b>
RM	Roma	Via del Corso 226	00186	Digitale	Server Farm
VR	Verona	Via Enrico Fermi, 4	37135	Digitale	Server Farm
BG	Pedrengo	Viale F.lli Kennedy, 21	24066	Digitale	Server Farm

**Scheda Tecnica: PULSE****REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE TECNICHE</b>	<b>SUPPORTI</b>
AR	Arezzo	Via Piero Calamandrei, 255	52100	Digitale	Server Farm
MI	Assago	Strada 3 Palazzo B/	20057	Digitale	Server Farm
FC	Forlì	Corso della Repubblica, 14	47121	Digitale	Server Farm
GO	Gorizia	Corso Verdi, 104	34170	Digitale	Server Farm
LU	Viareggio	Piazza Dante Alighieri, 4	55049	Digitale	Server Farm
TV	Montebelluna	Via Feltrina sud, 250	31044	Digitale	Server Farm
VR	Verona	Via Enrico Fermi, 4	37135	Digitale	Server Farm
VI	Vicenza	Via Battaglione Framarin, 18	36100	Digitale	Server Farm

# SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO

Banca dei Territori

## DOCUMENTO DESCRITTIVO

Tipo Impianto	Sistema di registrazione telefonica, Sibilla All-In-One, per registrazione chiamate effettuate con telefoni mobili in dotazione ai gestori. La tecnica utilizzata sfrutta la conferenza telefonica a 3 partecipanti, Recorder, Gestore e Cliente.
Caratteristiche tecniche	<p>Flusso ISDN standard Euro 30 canali monodirezionali, solo entranti. Le linee sono abilitate alla ricezione delle chiamate da parte del Recorder, non all'effettuazione di chiamate da questi. Consente un totale di 30 chiamate/registrazioni contemporanee. All'arrivo di una chiamata, la scheda IVR, funzionante come TE, risponde. La scheda di registrazione NICE, ne registra audio e segnalazione.</p> <p>Il sistema di risposta e registrazione è un server hardware, le cui caratteristiche principali sono:</p> <p>Media di registrazione: Hard Disk interno in Raid 1 + HS Alimentazione: Alimentatori ridondati Schede di rete: in configurazione ridondata Numero massimo di canali registrati: 30 contemporanei</p>
Ubicazione	c/o CED Moncalieri, Sala CCM-M109, Rack ZJ58, RU 5
Supporti	Hard Disk interno in configurazione RAID 1 + HS per buffer a breve termine (1 anno c.a.) e Storage di Parma per conservazione a lungo termine delle registrazioni.
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni. In caso di specifica previsione normativa che deroga tale termine, si provvede alla anticipata cancellazione delle registrazioni.
Modalità di registrazione e riascolto.	<p>Il sistema consente di registrare le telefonate effettuate/ricevute sui cellulari aziendali tramite l'attivazione del sistema IVR attivo sito presso il CED di Moncalieri. Il sistema inoltre trasferisce le registrazioni, tramite i server Sibilla, per l'archiviazione in appositi archivi di <i>storage</i> dotati di sistemi di protezione e <i>backup</i> localizzati presso <i>server farm</i> di Parma.</p> <p>Nella fase di riascolto delle telefonate la ricerca della telefonata avviene tramite un software Web (Saraweb) previo inserimento nell'apposita maschera, dei parametri identificativi (data inizio/fine del periodo di ricerca, ora inizio/fine del periodo di ricerca etc). Il sw web per la ricerca ed il riascolto è integrato con i Sistemi di Sicurezza Informatica (SWA2) e consente l'accesso esclusivamente alle persone abilitate. L'autenticazione e le credenziali di accesso sono garantite tramite SSO (Single Sign On).</p>

SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO

Banca dei Territori

DOCUMENTO DESCRITTIVO

<p>Modalità di registrazione e riascolto.</p>	<p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>
---	--

SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO

Intesa Sanpaolo  
DIVISIONE IMI CORPORATE & INVESTMENT BANKING (IMI CIB)

Strutture di Business

DOCUMENTO DESCRITTIVO

Tipo Impianto	Piattaforme di registrazione Nice Trading Recording versione R6 e versione 6.6.10 su apparati Server: DELL POWEREDGE R.6.3.0.
Caratteristiche tecniche	Sistema di Registrazione digitale in VOIP
Ubicazione	Sistema ubicato presso lo stabile di Piazza della Scala/Largo Mattioli nei locali tecnici di Intesa Sanpaolo, con archiviazione in appositi storage dotati di sistemi di protezione e backup localizzati in Server Farm di Intesa Sanpaolo a Settimo e Moncalieri. Soluzione Target: In Server Farm presso To-Moncalieri / Parma
Supporti	In Share di rete su Hard Disk presso Server Farm, gestita da gruppi lavorativi Intesa Sanpaolo (Sistemi di base)
Termini di conservazione	Secondo normativa tempo per tempo vigente: di norma ad oggi 10 anni dalla data di estinzione massima attesa della tipologia di contratto.
Modalità di registrazione e riascolto.	<p>La ricerca della telefonata avviene secondo procedura, mediante parametri identificativi richiesti. L'accesso è consentito attraverso chiavi digitali (Password).</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti, controparti e/o Organismi di vigilanza" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>



**Scheda Tecnica: IMI CIB Strutture di Business facenti capo all'Area di Coordinamento Global Banking and Markets**

				<b>REGISTRAZIONI DEGLI ORDINI TELEFONICI</b>	
<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE TECNICHE</b>	<b>SUPPORTI</b>
MI	Milano	Largo Mattioli, 3	20121	Digitale	Server Farm

SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO

Intesa Sanpaolo  
AREA DI GOVERNO CHIEF FINANCIAL OFFICER (CFO)

DOCUMENTO DESCRITTIVO

Tipo Impianto	Piattaforma di registrazione Nice Trading Recording versione 6.6.10 su apparati Server: DELL POWEREDGE R.6.3.0.
Caratteristiche tecniche	Sistema di Registrazione digitale in VOIP.
Ubicazione	Sistema ubicato presso lo stabile di Piazzetta Giordano dell'Amore, 3 nei locali tecnici di Intesa Sanpaolo, con archiviazione in appositi storage dotati di sistemi di protezione e backup localizzati in Server Farm di Intesa Sanpaolo a Settimo e Moncalieri  Soluzione Target: In Server Farm presso To-Moncalieri / Parma
Supporti	In Share di rete su Hard Disk presso Server Farm, gestita da gruppi lavorativi Intesa Sanpaolo (Sistemi di base)
Termini di conservazione	Secondo normativa tempo per tempo vigente: di norma ad oggi 10 anni dalla data di estinzione massima attesa della tipologia di contratto.
Modalità di registrazione e riascolto.	La ricerca della telefonata avviene secondo procedura, mediante parametri identificativi richiesti. L'accesso è consentito attraverso chiavi digitali (Password).  Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti, controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.

**Scheda Tecnica: Area CFO**

<b>Scheda Tecnica: Area CFO</b>				<b>REGISTRAZIONI DEGLI ORDINI TELEFONICI</b>	
<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE TECNICHE</b>	<b>SUPPORTI</b>
MI	Milano	Piazzetta Giordano Dell'Amore, 3	20121	Digitale	Server Farm

## SISTEMI DI REGISTRAZIONE DEI CANALI AUDIO

Intesa Sanpaolo:

DIVISIONE IMI CORPORATE & INVESTMENT BANKING (IMI CIB)

Strutture di Business con operatività rilevante ai fini del Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE

### AREA DI GOVERNO CFO

Strutture che partecipano alla contribuzione del tasso Euribor, strutture di business con operatività rilevante ai fini del Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e/o strutture operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE

## STRUMENTI DI WEB COLLABORATION SOGGETTI A RECORD KEEPING

### DOCUMENTO DESCRITTIVO

(tecnologia comune a tutte le risorse con operatività rilevante)

Tipo impianto	Cisco Webex – Theta Lake – Portale Web Theta Lake  Sono esclusi da questo Documento Descrittivo i seguenti strumenti di lavoro: sistemi informatici finalizzati all'esercizio delle attività assegnate quali la <i>posta elettronica server Outlook</i> (compresi gli account collegati ad un info-provider) e gli <i>strumenti di messaggistica istantanea e chat autorizzati in base alla normativa interna</i> in vigore quali, ad oggi: Bloomberg, Fxt Dealing, Refinitiv Messenger e WebIce.
Caratteristiche tecniche	Theta Lake soluzione SaaS
Ubicazione	Cloud Theta Lake in UE
Supporti di registrazione	NAS su cloud Theta Lake in UE
Termine di conservazione	Secondo normativa tempo per tempo vigente: di norma ad oggi 10 anni dalla data di estinzione massima attesa della tipologia di contratto.
Modalità di registrazione e riascolto.	La soluzione di registrazione archivia la traccia audio delle Videochiamate eseguite mediante la soluzione di collaboration Cisco Webex tramite una soluzione cloud, sempre di tipo SaaS, il cui fornitore è Theta Lake.  La soluzione Theta Lake permette l'archiviazione delle registrazioni, secondo quanto previsto dalla normativa vigente, in modalità protetta e fornisce la possibilità di ricercare puntualmente ogni contatto.  Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

Intesa Sanpaolo:  
DIVISIONE IMI CORPORATE & INVESTMENT BANKING (IMI CIB)  
Strutture di Business con operatività rilevante ai fini del  
Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e operanti in attività finanziarie e/o  
servizi d'investimento ai sensi della Direttiva 2014/65/UE

AREA DI GOVERNO CFO  
Strutture che partecipano alla contribuzione del tasso Euribor, strutture di business con operatività rilevante  
ai fini del Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e/o strutture di business  
operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE

### SMARTPHONE AZIENDALI

DOCUMENTO DESCRITTIVO  
(tecnologia comune a tutte le risorse con operatività rilevante)

Tipo impianto	Installazione APP Unigy Mobile Client ed attivazione della stessa tramite licenziamento univoco mensile da parte fornitore IPC
Caratteristiche tecniche	L'applicazione installata sui telefoni cellulari abilita l'utilizzo dei servizi erogati della centrale telefonica di trading presso i data center di Intesa San Paolo.
Ubicazione	App disponibile sugli store ufficiali (es. Play Store) scaricata sul device aziendale tramite Mobile Device Manager aziendale Intesa San Paolo
Supporti di registrazione	n/a
Termine di conservazione	Secondo normativa tempo per tempo vigente: di norma ad oggi 10 anni dalla data di estinzione massima attesa della tipologia di contratto. In particolare, l'applicazione non conserva i dati delle conversazioni in quanto è utilizzata solo ai fini di comunicazione con la centrale telefonica di trading presso i data center di Intesa San Paolo. La centrale telefonica, tra gli altri servizi, eroga quello della registrazione delle conversazioni voce e oltre a mantenere il dato sui sistemi di registrazione interni alla centrale lo esporta anche a PTR ai fini DFA MIFID II.
Modalità di registrazione e riascolto.	La ricerca della telefonata avviene secondo procedura, mediante parametri identificativi richiesti. L'accesso è consentito attraverso chiavi digitali (Password).  Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti, controparti e/o Organismi di vigilanza" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

### DIVISIONE IMI CORPORATE & INVESTMENT BANKING (IMI CIB)

Risorse in servizio presso Strutture di Business con operatività rilevante ai fini del Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e/o operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE

### AREA DI GOVERNO CFO

Strutture che partecipano alla contribuzione del tasso Euribor, strutture di business con operatività rilevante ai fini del Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e/o strutture di business operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE

## MICROSOFT TEAMS E SMARTPHONE AZIENDALI

### DOCUMENTO DESCRITTIVO

(tecnologia comune a tutte le risorse con operatività rilevante)

Tipo Impianto	Microsoft Teams App "Real Time Mobile" + Portale SaaS by Habble srl
Caratteristiche tecniche	Sviluppo custom che utilizza le graph API di Microsoft per scaricare le informazioni necessarie.  Applicazione per Smartphone con AndroidOS DB PostgreSQL su servizio Amazon RDS, criptato con l'utilizzo di una chiave a 256bit gestita tramite Amazon KMS
Ubicazione	Cloud Microsoft in UE  App locale su Smartphone DB su cloud AWS a Francoforte (UE)
Supporti	Invio delle registrazioni a PTR
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 5 anni
Modalità di registrazione dei metadati	Il sistema consente di registrare - i metadati inerenti alle comunicazioni non registrate intercorse mediante l'applicativo di work collaboration Teams, tra cui data inizio/fine della comunicazione, fuso orario, identificativo operatore di business coinvolto e identificativo dei partecipanti;  - i metadati inerenti alle comunicazioni non registrate intercorse mediante cellulare aziendale, sia orali sia via sms, tra cui data inizio/fine della comunicazione, fuso orario, identificativo operatore di business coinvolto e identificativo dei partecipanti.

## Scheda esplicativa – processi di Record Keeping

DIVISIONE IMI CORPORATE & INVESTMENT BANKING (IMI CIB) E AREA DI GOVERNO CHIEF FINANCIAL OFFICER

### A. RECORD-KEEPING DEI SISTEMI E DEI CANALI DI COMUNICAZIONE

Le Associated Person (e le risorse che partecipano alla contribuzione del tasso Euribor) con operatività rilevante ai fini del Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) e/o le strutture operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE hanno a disposizione sistemi e canali di comunicazione oggetto di tracciatura che devono usare al fine di garantire l'archiviazione e monitoraggio delle comunicazioni lavorative rilevanti ai sensi della normativa applicabile. I sistemi e i canali di comunicazione oggetto di tracciatura sono, tra l'altro, i seguenti:

- Piastre telefoniche della linea fissa anche laddove disponibile attraverso un emulatore sul pc e/o sullo smartphone aziendale;
- Posta elettronica server Outlook (compresi gli account collegati ad un info-provider);
- Strumenti di messaggistica istantanea e chat autorizzati in base alla normativa interna in vigore quali, ad esempio: Bloomberg, Fxt Dealing, Refinitiv Messenger e WebIce;
  - o Bloomberg: corporate mail, allegati delle mail, chat ed allegati delle chat associate alle utenze Bloomberg;
  - o FXT Messenger: messaggi istantanei;
  - o Eikon Messenger: messaggi istantanei (Reuters);
  - o WebIce: comunicazioni effettuate sulla piattaforma;
- Registro Ordini;
- Agende Salesforce.

L'elenco sopra può essere oggetto di aggiornamento in base alle tecnologie di volta in volta recepite ai sensi della normativa interna applicabile.

Inoltre, le Associated Person (e le risorse che partecipano alla contribuzione del tasso Euribor) – e dal 2025 le strutture operanti in attività finanziarie e/o servizi d'investimento ai sensi della Direttiva 2014/65/UE – hanno a disposizione uno strumento di "work collaboration" (Webex), ulteriore a Teams, che viene assoggettato a record-keeping e monitoraggio, da utilizzare in alternativa agli altri canali registrati per tutte le comunicazioni "business related", sia con interlocutori interni ad ISP che esterni.

Nel caso di utilizzo di Webex, gli utenti interessati sono chiamati a rispettare le seguenti regole:

- obbligo di creare dall'applicazione un invito da trasmettere ai propri interlocutori per garantire il record-keeping della comunicazione "business related";
- divieto di utilizzare link di accesso a strumenti di "work collaboration" inviati da interlocutori esterni; in questo caso l'operatore può in alternativa collegarsi via telefono fisso (piastre), affinché la conversazione venga registrata.

Teams resta utilizzabile per comunicazioni business related registrate a iniziativa dell'operatore, e per le comunicazioni non "business related", per cui vengono registrati e monitorati i metadati (data, ora, fuso orario di inizio e fine della conversazione, informazioni sui partecipanti alla comunicazione), come meglio dettagliato ai sensi delle Regole interne e delle Guide di Processo applicabili.

## B. RECORD-KEEPING DELLE COMUNICAZIONI "VOICE" TRAMITE SMARTPHONE

È previsto il rilascio sugli smartphone aziendali assegnati alle strutture registrate (e alle risorse che partecipano alla contribuzione del tasso Euribor) di una applicazione aggiuntiva (Unigy Mobile Client) individuata come canale da utilizzare per registrare le chiamate "business related" in entrata e in uscita.

## C. RECORD-KEEPING DEI METADATI

Sono inoltre oggetto di tracciatura:

- i metadati inerenti alle comunicazioni non registrate intercorse mediante l'applicativo di work collaboration Teams, tra cui data inizio/fine della comunicazione, fuso orario, identificativo operatore di business coinvolto e identificativo dei partecipanti;
- i metadati inerenti alle comunicazioni non registrate intercorse mediante cellulare aziendale, sia orali sia via sms, tra cui data inizio/fine della comunicazione, fuso orario, identificativo operatore di business coinvolto e identificativo dei partecipanti.

## D. CONTROLLI E MONITORAGGIO DELLE COMUNICAZIONI

Come previsto dalle vigenti regole in materia, ISP ha attivato controlli interni sulle comunicazioni per accertare il rispetto dei requisiti di record-keeping e di condotta previsti dalle normative applicabili, nonché ha attivato specifiche regole finalizzate a monitorare eventuali tentativi di spostamento delle comunicazioni orali e scritte al di fuori dei canali sottoposti a registrazione. In particolare, sono state create delle query all'interno del sistema di monitoraggio delle comunicazioni, NICE, volte ad intercettare questa tipologia di comportamento.

## E. ARCHIVIAZIONE

In tema di archiviazione, si specifica che le registrazioni delle comunicazioni orali e scritte:

- sono mantenute all'interno della UE anche per gli utenti extra UE;
- vengono conservate in modo conforme a quanto previsto tempo per tempo in materia: di norma ad oggi 10 anni dalla data di estinzione massima attesa della tipologia di contratto.

## F. INIZIATIVE DEGLI ORGANISMI DI VIGILANZA

Ai sensi delle Regole in essere, ISP è tenuta a fornire prontamente copia delle comunicazioni delle strutture di business registrate ai competenti Organismi di Vigilanza, europei ed extra-europei, al fine di dimostrare la conformità della Banca agli obblighi di record-keeping e di diligent supervision.



## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

Fideuram Intesa Sanpaolo Private Banking:  
Assistenza Rete e Clienti Contact Center Clienti e Reti  
Banca Diretta - Contact Center, Active Clients Trading e Servizi di Trading (Execution Desk di Trading Evoluto)

### DOCUMENTO DESCRITTIVO

Tipo Impianto	A.S.C.
Caratteristiche tecniche	<p>Apparati A.S.C., Windows, Cisco e DELL Apparati di registrazione EVoIP Marathon ASC su server Windows situati nelle server farm ISP. I telefoni hanno una configurazione tale per cui i pacchetti di rete vengono duplicati e inviati ad un apparato CUBE ( Cisco Unified Border Element ) che ha una interfaccia di collegamento verso i server di registrazioni siti nelle server farm ISP di Torino e Parma.</p> <p>Le conversazioni vengono così archiviate localmente sui server di registrazione ASC, questi scaricano la cache locale su server Windows denominati IAS e ogni notte vengono dapprima riversate su apparati NAS e quindi le registrazioni vengono archiviate definitivamente su sistemi storage persistenti DELL ( piattaforma ECS ), in modalità WORM.</p> <p>Tutte le registrazioni sono crittografate e accessibili al riascolto solo con applicazione ASC Powerplay che ne consente la ricerca tramite accesso profilato utilizzando una username ed una password, calcolata da un algoritmo.</p>
Ubicazione	Impianti custoditi nelle server farm di Intesa Sanpaolo
Supporti	Registrazione su dischi locali, di tipo NAS e archiviazione worm su ECS.
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di riascolto	<p>L'accesso alle registrazioni avviene tramite l'utilizzo del software ASC Power Play.</p> <p>L'accesso avviene in due step. Viene creata una password da parte di una risorsa abilitata con profilo Admin/Creatore che consente ad un'altra risorsa, abilitata con apposito profilo, di poter ascoltare la registrazione telefonica.</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO/VIDEO

BANCA DIRETTA FIDEURAM – Contact Center

DOCUMENTO DESCRITTIVO

Tipo impianto	Cisco Webex – Theta Lake – Portale Web Theta Lake
Caratteristiche tecniche	Theta Lake soluzione SaaS
Ubicazione	Cloud Theta Lake in UE
Supporti di registrazione	NAS su cloud Theta Lake in UE
Termine di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di registrazione e riascolto.	<p>La soluzione di registrazione archivia la traccia audio e video delle Videochiamate eseguite mediante la soluzione di collaboration Cisco Webex tramite una cloud, sempre di tipo SaaS, il cui fornitore è Theta Lake. La componente video viene attivata solo lato cliente e non per il dipendente.</p> <p>La soluzione Theta Lake permette l'archiviazione delle registrazioni, secondo quanto previsto dalla normativa vigente, in modalità protetta e fornisce la possibilità di ricercare puntualmente ogni contatto.</p> <p>In caso di necessità, il riascolto avviene mediante la FDI che si mette in contatto con la struttura GT che ha in gestione la piattaforma Cloud. Questa si occupa di effettuare la ricerca del file e di depositarlo su un repository posizionato su infrastruttura Banca il cui accesso è limitato al richiedente e alla funzione IT. Il dipendente che ha eseguito la Webex ha la possibilità di procedere in autonomia a rivedere e riascoltare il contenuto registrato. In caso di necessità viene contattata la struttura IT preposta.</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

**Fideuram Intesa Sanpaolo Private Banking: Assistenza Rete e Clienti Contact Center Clienti e Reti Banca Diretta Contact Center Trading**

**REGISTRAZIONI DEGLI ORDINI TELEFONICI**

PROVINCIA	COMUNE	INDIRIZZO SEDE	CAP	CARATTERISTICHE TECNICHE	SUPPORTI
MI	Milano	Via Melchiorre Gioia 22	20124	Digitale	Server Farm
RM	Roma	Piazzale G. Douhet 31	00143	Digitale	Server Farm

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

Fideuram Intesa Sanpaolo Private Banking  
FINANZA E TESORERIA  
Portafoglio di Proprietà – Strutturazione Prodotti – Tesoreria e Cambi  
MIDDLE OFFICE E EXECUTION DESK  
Execution Desk

### DOCUMENTO DESCRITTIVO

Tipo Impianto	Piattaforma di registrazione Nice Trading Recording versione 6.6.10 su apparati Server: DELL POWEREDGE R.6.3.0
Caratteristiche tecniche	Sistema di Registrazione digitale in VOIP
Ubicazione	Sistema ubicato a Milano, in Piazzetta Giordano dell'Amore 3 presso locali tecnici di Intesa Sanpaolo, con archiviazione presso appositi storage dotati di sistemi di protezione e backup localizzati in Server Farm di Intesa a Settimo Torinese e Moncalieri.
Supporti	In Share di rete su Hard Disk presso Server Farm, gestita da gruppi lavorativi Intesa Sanpaolo (Sistemi di base).
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni.
Modalità di registrazione e riascolto.	<p>La ricerca della telefonata avviene secondo procedura, dei parametri identificativi richiesti. L'accesso è consentito attraverso chiavi digitali (Password).</p> <p>I riascolti che avvengono in sede si svolgono nell'ufficio del presidio telefonia di GDA oppure per le utenze storiche Fideuram tramite la propria postazione di lavoro con chiavi di utenze e pwd.</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti, controparti e/o Organismi di vigilanza" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

**Scheda Tecnica: Fideuram Intesa Sanpaolo Private Banking FINANZA E TESORERIA**  
Portafoglio di Proprietà – Strutturazione Prodotti – Tesoreria e Cambi  
**MIDDLE OFFICE E EXECUTION DESK - Execution Desk**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE TECNICHE</b>	<b>SUPPORTI</b>
MI	Milano	Piazzetta Giordano Dell'Amore, 3	20121	Digitale	Server Farm

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

Intesa Sanpaolo Private Banking (ISPB): Rete e Advisory  
Fideuram Asset Management SGR: Gestioni Patrimoniali Individuali (GPI)

### DOCUMENTO DESCRITTIVO

Tipo Impianto	Componente IVR attiva e componente passiva di registrazione Audio NICE NTR
Caratteristiche tecniche	<p>N° 2 server NICE NTR in HA N° 2 Flussi ISDN standard Euro 30 canali bidirezionali (consente un totale di 60 chiamate/registrazioni contemporanee).</p> <p>Componente IVR attiva lato ISDN per Conference termination con l'Utente.</p> <p>Componente passiva di registrazione Audio: NICE NTR Media di registrazione: Hard Disk interno in Raid 1 Numero massimo di canali registrati: 60 contemporanei Ore di registrazione: 30.000 ore circa su HD</p>
Ubicazione	C/o il Data Center di Intesa Sanpaolo di Moncalieri in appositi locali tecnici
Supporti	Hard Disk NICE NTR interno in configurazione RAID 1 e archiviazione/backup su Storage Parma
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 anni
Modalità di registrazione e riascolto.	<p>Il sistema consente di registrare le telefonate effettuate/ricevute sui cellulari aziendali tramite l'attivazione del sistema IVR attivo sito presso il Data Center di Intesa Sanpaolo. Il sistema inoltre trasferisce le registrazioni, tramite i server Sibilla, per l'archiviazione in appositi archivi di storage dotati di sistemi di protezione e backup localizzati presso server farm di Intesa Sanpaolo.</p> <p>Nella fase di riascolto delle telefonate la ricerca della telefonata avviene tramite un software Web (Saraweb) previo inserimento nell'apposita maschera, dei parametri identificativi (data inizio/fine del periodo di ricerca, ora inizio/fine del periodo di ricerca etc). Il sw web per la ricerca ed il riascolto è integrato con i Sistemi di Sicurezza Informatica (SWA2) e consente l'accesso esclusivamente alle persone abilitate. L'autenticazione e le credenziali di accesso sono garantite tramite SSO (Single Sign On).</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti e/o controparti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona da lui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

## SISTEMI DI REGISTRAZIONE DEL CANALE AUDIO

ISPB: Rete e Advisory  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)

### DOCUMENTO DESCRITTIVO

Tipo Impianto	SERVER RETIA
Caratteristiche tecniche	<p>RECORDER RETIA: server in ambiente VMware ridondato sui data center di Moncalieri e Parma</p> <p>Media di registrazione: Spazio archiviazione VMware</p> <p>Numero massimo di utenze registrabili: 1600</p> <p>Ore di registrazione: 30.000 ore circa su spazio archiviazione VMware</p> <p>Sibilla: server in ambiente VMware ridondato sui data center di Moncalieri e Parma</p>
Ubicazione	<p>RECORDER RETIA Presso i Data Center Intesa Sanpaolo</p> <p>Server Sibilla Presso i Data Center Intesa Sanpaolo</p> <p>Gli impianti sono custoditi in appositi locali tecnici.</p>
Supporti	Spazio archiviazione VMware e StorageParma
Termini di conservazione	Secondo normativa tempo per tempo vigente: ad oggi 10 i
Modalità di registrazione e riascolto.	<p>Il sistema consente di effettuare automaticamente le registrazioni di tutte le telefonate in entrata o in uscita che transitano su numeri telefonici appositamente abilitati e opportunamente contrassegnati. Il sistema inoltre trasferisce le registrazioni, tramite i server Sibilla, per l'archiviazione in appositi archivi di storage dotati di sistemi di protezione e backup localizzati presso server farm di Intesa Sanpaolo.</p> <p>Nella fase di riascolto delle telefonate la ricerca della telefonata avviene tramite un software Web (Saraweb) previo inserimento nell'apposita maschera, dei parametri identificativi (data inizio/fine del periodo di ricerca, ora inizio/fine del periodo di ricerca etc).</p> <p>Il software web per la ricerca ed il riascolto è integrato con i Sistemi di Sicurezza Informatica (SWA2) e consente l'accesso esclusivamente alle persone abilitate. L'autenticazione e le credenziali di accesso sono garantite tramite SSO (Single Sign On).</p> <p>Il processo sopra descritto è relativo al "riascolto ad iniziativa della Banca in tutti i casi di contestazione su una transazione ad opera di clienti" e prevede la partecipazione dell'addetto che ha materialmente curato l'operazione o, in caso di sua assenza, di altra persona dalui incaricata, con facoltà di farsi assistere da un rappresentante sindacale delle OO.SS. firmatarie del presente accordo.</p>

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZION  
IDEGLI ORDINI  
TELEFONICI**

PROVINCIA	COMUNE	INDIRIZZO SEDE	CAP	CARATTERISTICHE ETECNICHE	SUPPORTI
TO	Moncalieri	Corso Savona, 58	10024	Digitale	Server Farm
AN	Ancona	Via Cialdini, 2 angolo Corso Stamira	60122	Digitale	Server Farm
BA	Bari	Piazza Luigi di Savoia, 16	70121	Digitale	Server Farm
CZ	Catanzaro	Piazza Grimaldi, sn	88100	Digitale	Server Farm
AN	Civitanova Marche	Corso Umberto I, 16	62012	Digitale	Server Farm
CS	Cosenza	Corso Umberto I, 17/A	87100	Digitale	Server Farm
FG	Foggia	Corso V. Emanuele II, 35	71121	Digitale	Server Farm
LE	Lecce	Piazza Mazzini 59	73100	Digitale	Server Farm
PU	Pesaro	Via Gagarin, 216	61122	Digitale	Server Farm
PE	Pescara	Corso V. Emanuele, 68	65122	Digitale	Server Farm
RC	Reggio Calabria	Via Foti, 3	89125	Digitale	Server Farm
AP	S. Benedetto	Via Risorgimento, 71	63039	Digitale	Server Farm
TA	Taranto	Corso Umberto I, 69	74123	Digitale	Server Farm
BO	Bologna	Via Francesco Rizzoli, 1/2	40124	Digitale	Server Farm
BO	Bologna	Via Farini, 22	40124	Digitale	Server Farm
BO	Bologna	Via Farini, 22	40124	Digitale	Server Farm
BO	Casalecchio di Reno	Via Ronzani, 21	40033	Digitale	Server Farm



**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
FE	Ferrara	Via Correggiari, 1	44100	Digitale	Server Farm
FC	Forlì	Via J. Allegretti angolo Piazza Saffi	47121	Digitale	Server Farm
BO	Imola	Via Cavour, 64	40026	Digitale	Server Farm
MO	Modena	Via dell'Università, 33	41121	Digitale	Server Farm
MO	Modena	Via Sant'Agostino, 24	41121	Digitale	Server Farm
PR	Parma	Piazza Cesare Battisti, 1	43121	Digitale	Server Farm
PC	Piacenza	Via Verdi, 48	29121	Digitale	Server Farm
RA	Ravenna	Via G. Rasponi, 2	48100	Digitale	Server Farm
RE	Reggio Emilia	Galleria Cavour, 2	42121	Digitale	Server Farm
RN	Rimini	Via Guerrazzi, 7	47921	Digitale	Server Farm
AV	Avellino	Via De Sanctis, 2	83100	Digitale	Server Farm
CA	Cagliari	Viale Bonaria c/o Palazzo CIS	9125	Digitale	Server Farm
CE	Caserta	Via C. Battisti, 49 angolo Piazza Generale d'Amico	81100	Digitale	Server Farm
FR	Frosinone	Piazza F. Fellini, 4	3100	Digitale	Server Farm
NA	Napoli	Via Toledo, 177/178	80134	Digitale	Server Farm
NA	Napoli	Via Riviera di Chiaia, 131	80122	Digitale	Server Farm
NA	Napoli	Via Toledo, 177/178	80132	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
RM	Roma	Via Ferdinando di Savoia, 8	196	Digitale	Server Farm
RM	Roma	Via Dei Condotti, 11	187	Digitale	Server Farm
RM	Roma	Via Del Corso, 226	186	Digitale	Server Farm
RM	Roma	Piazzale Douhet 31	143	Digitale	Server Farm
RM	Roma	Via Alessandro Torlonia, 15	161	Digitale	Server Farm
SA	Salerno	Via Fieravecchia, 3 angolo Corso V. Emanuele, 81	84122	Digitale	Server Farm
NA	San Giuseppe Vesuviano	Via XX Settembre, 52	80047	Digitale	Server Farm
SS	Sassari	Piazza d'Italia, 19	7100	Digitale	Server Farm
BG	Bergamo	Portici Sentierone 32	24121	Digitale	Server Farm
BG	Bergamo	Via Gennaro Sora, 12	24121	Digitale	Server Farm
CA	Brescia	Via Trieste, 8	25121	Digitale	Server Farm
BG	Bergamo	Via Sora 9	24121	Digitale	Server Farm
BG	Bergamo	Via Camozzi 39	24121	Digitale	Server Farm
VA	Busto Arsizio	Via San Gregorio, 1	21052	Digitale	Server Farm
CO	Como	Via Rubini, 6 - scala C	22100	Digitale	Server Farm
CO	Como	Via Rubini, 6 - scala B	22100	Digitale	Server Farm
LC	Lecco	Via Cavour, 67	23900	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
MI	Legnano	Corso Italia, 54	20025	Digitale	Server Farm
VA	Varese	Via Marconi, 3	21100	Digitale	Server Farm
VA	Varese	Via Marconi 3	22100	Digitale	Server Farm
BS	Brescia	via Paganora, 2	25121	Digitale	Server Farm
CR	Crema	Via Racchetti, 1	26013	Digitale	Server Farm
CR	Cremona	Via Lanaioli, 2	26100	Digitale	Server Farm
LO	Lodi	Via Volturmo, 13	26900	Digitale	Server Farm
MN	Mantova	Via Frattini,7	46100	Digitale	Server Farm
MI	Melzo	Via Magenta, 2/4	20066	Digitale	Server Farm
MB	Monza	Via Vittorio Emanuele II, 26	20900	Digitale	Server Farm
MB	Monza	Via San Paolo, 1	20900	Digitale	Server Farm
PV	Pavia	Via Cesare Battisti, 16/B	27100	Digitale	Server Farm
PV	Pavia	Corso strada Nuova, 61/63	27100	Digitale	Server Farm
PV	Pavia	VIALE C.BATTISTI, 16-B	27100	Digitale	Server Farm
PV	Vigevano	Corso V. Emanuele, 5	27029	Digitale	Server Farm
MI	Milano	Via Leopardi, 10	20123	Digitale	Server Farm
MI	Milano	Piazza Borromeo, 12	20123	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
MI	Milano	Foro Bonaparte, 24	20121	Digitale	Server Farm
MI	Milano	Corso di Porta Nuova 7	20121	Digitale	Server Farm
MI	Milano	Via Hoepli, 10	20121	Digitale	Server Farm
MI	Milano	Corso San Gottardo, 1	20136	Digitale	Server Farm
MI	Milano	Via Vittorio Veneto, 22	20124	Digitale	Server Farm
MI	Milano	Via Lovanio, 5	20121	Digitale	Server Farm
MI	Milano	Via San Nicolao angolo Corso Magenta, 32	20123	Digitale	Server Farm
MI	Milano	C.so Venezia, 54	20121	Digitale	Server Farm
VI	Bassano del Grappa	Piazza della Libertà, 17	20900	Digitale	Server Farm
BL	Belluno	Piazza Vittorio Emanuele II, 11	20900	Digitale	Server Farm
BZ	Bolzano	Via della Mostra, 7/A	27100	Digitale	Server Farm
VR	Cerea	Via Paride da Cerea, 1/3	27100	Digitale	Server Farm
VE	Chioggia	Calle Nordio Marangoni, 99	27100	Digitale	Server Farm
PD	Cittadella	Via Marconi, 11/13	27029	Digitale	Server Farm
TV	Conegliano	Via Carlo Rosselli, 10	31015	Digitale	Server Farm
VE	Mestre	Piazzetta Matter, 4	30174	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
PD	Padova	Corso Garibaldi, 22/26	35122	Digitale	Server Farm
PD	Padova	Corso Garibaldi, 22/26	35122	Digitale	Server Farm
PD	Piove Di Sacco	Via Garibaldi, 45	35028	Digitale	Server Farm
PN	Pordenone	Via Mazzini, 12	33170	Digitale	Server Farm
RO	Rovigo	Via Mazzini, 9/13	45100	Digitale	Server Farm
VE	San Donà di Piave	Via Battisti, 3	30027	Digitale	Server Farm
VI	Schio	Piazza Alessandro Rossi, 3	36015	Digitale	Server Farm
TN	Trento	Via Mantova, 19	38122	Digitale	Server Farm
TV	Treviso	Via Indipendenza, 16	31100	Digitale	Server Farm
TV	Treviso	Via Indipendenza, 16	31100	Digitale	Server Farm
TS	Trieste	Via Dante, 5	34122	Digitale	Server Farm
UD	Udine	Via Carducci, 5	33100	Digitale	Server Farm
VE	Venezia	San Marco 4216 (Campo Manin)	30124	Digitale	Server Farm
VR	Verona	Vicolo Ghiaia, 7	37122	Digitale	Server Farm
VI	Vicenza	Contrà del Monte, 11	36100	Digitale	Server Farm
CT	Catania	Viale Regina Margherita, 39	95125	Digitale	Server Farm
ME	Messina	Via Pellegrino, 26	98123	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
PA	Palermo	Via Mariano Stabile, 152	90139	Digitale	Server Farm
TO	Chieri	Piazza Cavour, 8	10023	Digitale	Server Farm
TO	Moncalieri	Via San Martino, 34	10024	Digitale	Server Farm
TO	Pinerolo	Piazza San Donato, sn	10064	Digitale	Server Farm
TO	Torino	Piazza Crimea, 1	10131	Digitale	Server Farm
TO	Torino	Torino P.zza San Carlo 156	10121	Digitale	Server Farm
TO	Torino	Via Monte di Pietà, 32	10122	Digitale	Server Farm
TO	Torino	Corso Stati Uniti, 17	10128	Digitale	Server Farm
AR	Arezzo	Via Cavour, 105	52100	Digitale	Server Farm
FI	Empoli	Via Pievano Rolando, 2	50053	Digitale	Server Farm
FI	Firenze	Via Bufalini, 6	50122	Digitale	Server Farm
FI	Firenze	Via Gramsci, 69	50132	Digitale	Server Farm
LU	Lucca	Via Di Poggio, 3	55100	Digitale	Server Farm
PG	Perugia	Strada Pian della Genna, 21/F	6128	Digitale	Server Farm
PT	Pistoia	Corso Gramsci, 8 A	51100	Digitale	Server Farm
PO	Prato	Viale della Repubblica, 247/249	59100	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
SI	Siena	Piazza Giacomo Matteotti, 34	53100	Digitale	Server Farm
TR	Terni	Corso Tacito 49 A	5100	Digitale	Server Farm
CN	Alba	Piazza Michele Ferrero, 1	12051	Digitale	Server Farm
CN	Alba	Via Teobaldo Calissano, 9	12051	Digitale	Server Farm
AL	Alessandria	Piazza Garibaldi, 58	15121	Digitale	Server Farm
AO	Aosta	Piazza E. Chanoux, 38	11100	Digitale	Server Farm
AT	Asti	Corso Dante, 4	14100	Digitale	Server Farm
BI	Biella	Via Italia, 17/C	13900	Digitale	Server Farm
NO	Borgomanero	Via Gozzano, 107	28021	Digitale	Server Farm
AL	Casale Monferrato	Via Magnocavallo, 17/A	15033	Digitale	Server Farm
CN	Cuneo	Via Roma, 13/B	12100	Digitale	Server Farm
CN	Saluzzo	VIA TORINO, 38/A	12037	Digitale	Server Farm
GE	Genova	Via Fieschi, 6	16121	Digitale	Server Farm
TO	Ivrea	Piazza Balla, 7	10015	Digitale	Server Farm
SP	La Spezia	Via Galilei, 2	19121	Digitale	Server Farm
CN	Mondovì	Piazzale Ellero, 10	12084	Digitale	Server Farm

**Scheda Tecnica: ISPB - Rete e Advisory;  
Fideuram Asset Management SGR: Gestioni Patrimoniali  
Individuali (GPI)**

**REGISTRAZIONI  
DEGLI ORDINI  
TELEFONICI**

<b>PROVINCIA</b>	<b>COMUNE</b>	<b>INDIRIZZO SEDE</b>	<b>CAP</b>	<b>CARATTERISTICHE E TECNICHE</b>	<b>SUPPORTI</b>
NO	Novara	Corso Cavour, 18	28100	Digitale	Server Farm
AL	Novi Ligure	Corso Marengo, 6	15067	Digitale	Server Farm
IM	San Remo	Corso Matteotti, 169	18038	Digitale	Server Farm
SV	Savona	CORSO ITALIA, 12	17100	Digitale	Server Farm
CN	Cuneo	Via Roma, 13/B	12100	Digitale	Server Farm
GE	Genova	Via Fieschi, 6	16121	Digitale	Server Farm
NO	Novara	Corso Cavour, 18	28100	Digitale	Server Farm
VB	Verbania	Piazza Aldo Moro, 8	28921	Digitale	Server Farm
VC	Vercelli	Via D. Alighieri angolo Via Mandelli	13100	Digitale	Server Farm
BA	Bari	Piazza Luigi di Savoia, 16	70121	Digitale	Server Farm
VI	Vicenza	Contrà del Monte, 11	36100	Digitale	Server Farm
VR	Verona	Via Anfiteatro 1, Verona	37121	Digitale	Server Farm
MI	Milano	Via Montebello 18, Milano	20121	Digitale	Server Farm



## SISTEMI DI DATA LOSS PREVENTION (DLP)

### DOCUMENTO DESCRITTIVO

(Apparato comune alle infrastrutture informatiche del Gruppo ISP volto a prevenire la perdita di informazioni)

Tipo Impianto	Software Microsoft Data Loss Prevention (DLP)
Caratteristiche tecniche	<p>Sistema digitale finalizzato alla mitigazione del rischio di perdita dei dati rilevanti per il Gruppo ed al rafforzamento dell'aderenza alle normative vigenti in tema di protezione dei dati (in particolare: GDPR).</p> <p>La soluzione di DLP individuata è finalizzata a migliorare le capacità di identificare violazioni nel trattamento dei dati aziendali, con l'obiettivo di prevenire la perdita di informazioni (data breach).</p>
Ubicazione	Servizio integrato nella piattaforma Microsoft Office 365, presente su ambiente distribuito (postazioni aziendali in dotazione agli utenti).
Supporti	PC Aziendali Device mobile aziendali Cloud Azure Microsoft aziendale
Termini di conservazione	Conforme alla normativa tempo per tempo vigente in materia, ad oggi 12 mesi.
Modalità di tracciatura e accesso	<p>La protezione del dato prevede l'individuazione ed il tracciamento delle sole violazioni di trattamento dei dati aziendali compiute dagli utenti, rispetto alle regole aziendali impostate.</p> <p>I dati tracciati saranno consultati solo in caso si verifichi un incidente con perdita di dati riservati e verranno mantenuti solo per il periodo strettamente necessario a tali scopi.</p> <p>L'accesso alle informazioni tracciate sarà consentito solo ad un ristretto e autorizzato numero di utenti (amministratori) congiuntamente ad Audit.</p> <p>L'autorizzazione è regolata dagli attuali processi aziendali, i quali prevedono l'approvazione da parte di un responsabile, la firma di una lettera di incarico in ottemperanza alla legislazione sulla privacy. Inoltre, l'incarico amministrativo viene periodicamente ricertificato a garanzia del principio del minimo privilegio.</p>

TRACCIATURA DELLE OPERAZIONI BANCARIE  
DOCUMENTO DESCRITTIVO

(Sistema comune a tutte le Società che tempo per tempo fanno parte del Gruppo ISP)

Caratteristiche di base

Caratteristiche tecniche	Base dati dipartimentale/BFD, ambiente dedicato collocato in infrastruttura standard. Prodotto standard di mercato. Previsto salvataggio di backup giornaliero secondo processi standard.
Termine di conservazione	24 mesi
Modalità accesso	Con riconoscimento ruoli e profili sistemistici secondo processi standard.

Dettagli tecnici *log* e flussi

Caratteristiche tecniche	Flussi di dati dipartimentali e host, generati e gestiti su infrastruttura standard Spediti e ricevuti mediante i processi e gli strumenti di trasferimento file standard.
Termine di conservazione	24 mesi a destinazione
Modalità accesso	Con riconoscimento ruoli e profili sistemistici secondo processi standard

## **Scheda esplicativa - tracciatura delle operazioni bancarie (descrizione del processo e caratteristiche tecniche delle elaborazioni).**

Ai fini della tracciatura delle operazioni bancarie come richiesto dal Provvedimento emesso dal Garante per la protezione dei dati personali:

1. per tutte le operazioni bancarie eseguite sui sistemi si verifica, anche in ambienti BFD, se sono da tracciare secondo le disposizioni del Provvedimento, ossia se trattano dati bancari di clienti soggetti alla normativa privacy vigente (persone fisiche come classificate in anagrafe clienti e ditte individuali);
2. le operazioni individuate in ambito al punto precedente sono registrate dalle singole procedure informatiche nelle basi dati, tutte in infrastrutture standard. Le informazioni registrate sono le informazioni richieste dal Provvedimento, ossia:
  - a. il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso (user di chi ha eseguito l'operazione);
  - b. la data e l'ora di esecuzione;
  - c. il codice della postazione di lavoro utilizzata o indirizzo IP da cui è stato effettuato l'accesso;
  - d. il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato (es.: codice fiscale, NDG, SNDG, p.iva, ecc...);
  - e. la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata - es. conto corrente, fido/mutuo, deposito titoli, numero identificativo del rapporto oggetto, filiale del rapporto, forma tecnica del rapporto;
3. giornalmente le operazioni vengono inviate in modo automatico, mediante infrastruttura di trasferimento file standard, a basi dati centralizzate che le conservano per i 24 mesi previsti dal Provvedimento. Tutta l'attività di estrazione, invio e ricezione è automatizzata;
4. Le strutture tecnologiche utilizzate sono standard e di mercato.  
Le ulteriori informazioni memorizzate sono le seguenti:
  - f. codice della banca/società in cui è eseguita l'operazione;
  - g. identificativo dell'applicazione utilizzata;
  - h. cognome e nome del soggetto che ha eseguito l'operazione;
  - i. banca/società di appartenenza del soggetto che ha eseguito l'operazione.

Nel caso in cui il soggetto che ha eseguito l'operazione sia un soggetto incaricato esterno alla banca/società:

- j. user del riferimento interno;
- k. cognome e nome del riferimento interno;
- l. ente di riferimento interno.

Nel caso in cui l'operazione sia indirizzata ad uno specifico identificativo di cliente o rapporto:

- m. super NDG/NSG del cliente oggetto dell'operazione;
- n. anagrafica del cliente oggetto dell'operazione;
- o. filiale di portafoglio;
- p. codice portafoglio;
- q. matricola gestore;
- r. cognome e nome gestore.

Nel caso in cui l'operazione non sia indirizzata ad uno specifico identificativo di cliente o rapporto, ma siano delle "ricerche massive":

- s. parametri di ricerca inseriti: quali l'insieme dei parametri inseriti che consentono di individuare il contenuto dei dati richiesti in estrazione.

Nel caso in cui l'operazione sia eseguita in ambiente BFD, oltre ai parametri di ricerca inseriti per l'estrazione:

- t. sorgente sulla quale sono presenti i dati;
- u. tipologia di sorgente dati in analisi;
- v. tipologia di operazione eseguita sulla sorgente dati;
- w. identificativi del database;
- x. nome della banca/società relativa al database, ove presente;

Le operazioni ricevute sono inserite nelle basi dati centralizzate, dove vengono conservate per 24 mesi;

5. reporting: sulla base dati è prevista la creazione di report con interfaccia standard di Business Intelligence, il cui accesso è consentito ai referenti della Funzione Privacy competente per la società secondo i ruoli ed i processi di autenticazione standard. Laddove l'accesso consenta la visualizzazione di dati bancari, tali accessi sono, a loro volta, tracciati secondo le modalità e le regole definite dal Provvedimento.

## Richiesta di convocazione del Comitato di Consultazione

Spettabili

Comitato di Consultazione

Delegazioni Sindacali di Gruppo

Intesa Sanpaolo

Ufficio Relazioni Industriali

-----  
Nome società

<indirizzo>

Oggetto: Accordo in materia di attuazione dell'art. 4 L n. 300/1970 - richiesta convocazione Comitato di Consultazione.

L'Azienda e/o le scriventi RR.SS.AA./Coordinatori RR.SS.AA. di ....., in adempimento alle previsioni del punto 3.A., 3.B., 3.C. e 3.D. dell'accordo in oggetto, avendo constatato in data odierna..... la possibile mancata rispondenza del contenuto della richiamata scheda/planimetria relativa a <sede società/filiale>, chiedono, in applicazione dell'articolo 3 del Protocollo delle Relazioni Industriali 14 aprile 2021, la convocazione del Comitato di Consultazione, secondo le regole e le finalità ivi previste.

Distinti saluti.