

## 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

premesso 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* tracciano 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*