Privacy Policy

Consiglio di Amministrazione di Banca Mediolanum S.p.A. del 29 Marzo 2022

1. PREMESSA e AMBITO

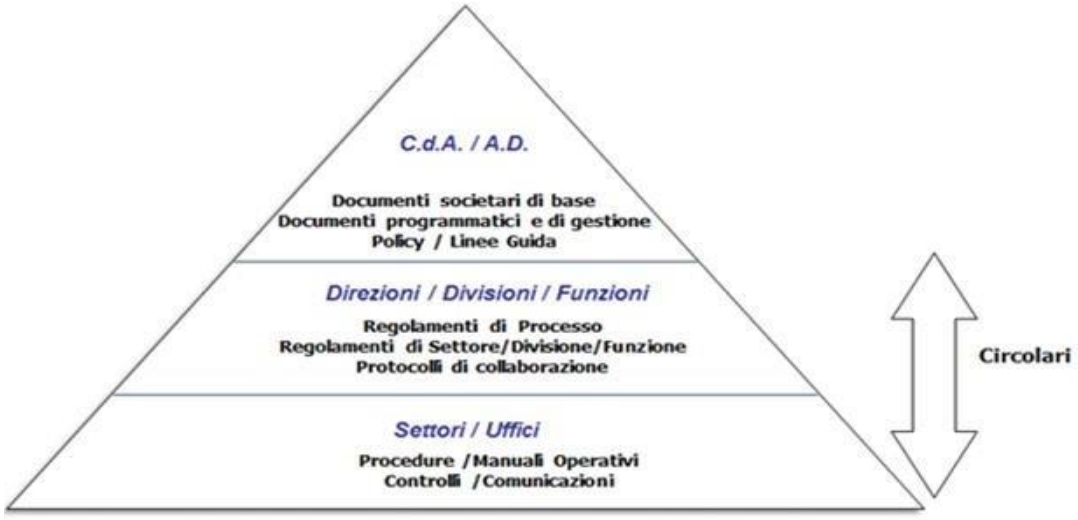
Il presente documento si propone di fornire una descrizione dei principi, in tema di privacy, adottati da Banca Mediolanum S.p.A. (nel seguito del documento anche “la Banca”), in qualità di società del Gruppo Bancario Mediolanum (nel seguito del documento “il Gruppo) e Capogruppo del Conglomerato Finanziario (nel seguito del documento anche “il Conglomerato”) per il presidio degli aspetti inerenti al trattamento dei dati personali, o appartenenti a categorie particolari, degli interessati (a titolo meramente esemplificativo e non esaustivo: clienti, dipendenti, fornitori e visitatori), in conformità al Regolamento UE 2016/679 “GDPR in Materia di Protezione dei Dati Personali” (di seguito anche “GDPR”), alla normativa nazionale vigente ed ai provvedimenti emessi dal Garante per la protezione dei dati personali (di seguito anche “il Garante”).

I principi richiamati nella presente policy trovano attuazione nei regolamenti di processo, nei quali saranno meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto degli adempimenti relativi alle normative in tema di tutela dei dati personali.

La Banca con il presente documento fornisce le linee guida e identifica i requisiti da rispettare per la corretta gestione dei dati personali, ciò al fine di assicurare che il trattamento di tali dati personali, appartenenti tra l’altro a categorie particolari e a dati relativi a condanne penali e reati, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei medesimi.

Il presente documento costituisce un primo livello (di vertice) nella piramide riportata nello schema seguente che raffigura il modello logico della normativa aziendale richiamato dalla policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna della Banca[1]

Figura 1. Modello della normativa aziendale



1 *Circolare n. 101/16 del 21/12/2016*

2. APPLICABILITÀ

2.1. DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Banca Mediolanum S.p.A. e trova diretta applicazione all'interno della stessa. I principi definiti si applicano a tutte le unità organizzative della Banca incluse nel perimetro di intervento.
Viene inoltre inviato per l'adozione – secondo un principio di proporzionalità e tenuto conto delle normative e specificità locali – alle Società facenti parte del Conglomerato.

Le Società estere applicano la presente policy fatto salvo il caso in cui la normativa locale abbia requisiti diversi e più stringenti.

2.2. RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità dell'Ufficio Privacy della Direzione Affari Societari, Legali e Contenzioso di Banca Mediolanum S.p.A.

3.DEFINIZIONI

"Trattamento": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

"Dato personale": qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

"Dati identificativi": i dati personali che permettono l'identificazione diretta dell'interessato.

"Dati appartenenti a categorie particolari": i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

"Dati relativi a condanne penali e reati": i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato

"Soggetto interessato": la persona fisica cui si riferiscono i dati personali.

Ai fini del presente documento, per le altre definizioni, si fa diretto riferimento alle definizioni di cui all'articolo 4 del GDPR e delle altre normative applicabili, di cui al capitolo 10 della presente policy.

4. RUOLI E RESPONSABILITÀ DEL PRESIDIO DELLA NORMATIVA PRIVACY

Il modello adottato per il presidio degli aspetti inerenti al trattamento dei dati personali,

appartenenti, tra l'altro, a categorie particolari e dati relativi a condanne penali e reati della clientela, dei dipendenti e dei fornitori prevede il coinvolgimento delle seguenti strutture aziendali di Banca Mediolanum Spa nei principali aspetti privacy:

- **Ufficio Privacy:** costituito all'interno della DivisioneAffari Legali, svolge e coordina tutti gli adempimenti previsti dalle normative in tema di privacy, per Banca Mediolanum e per alcune società del Conglomerato, in virtù di appositi contratti di servizio. In particolare:
  - provvede alle comunicazioni al Garante;
  - cura la redazione e l'aggiornamento delle lettere di nomina a responsabile, delle lettere di nomina a soggetto autorizzato e delle informative sul trattamento dei dati tenendo conto delle finalità indicate dalle funzioni aziendali interessate;
  - cura la gestione delle richieste dell'interessato inerenti i propri dati;
  - cura la gestione delle richieste relative al GDPR;
  - effettua la supervisione sulla formazione Privacy erogata ai dipendenti;
  - redige e aggiorna le informative e i consensi privacy;
  - fornisce la consulenza, in materia di privacy, a tutte le funzioni aziendali;
  - evade i reclami dei Clienti relativi alla privacy;
- **Ict:** cura il presidio delle misure di sicurezza previste dalle normative privacy e gli adempimenti previsti per la gestione degli amministratori di sistema.
- **Internal audit:** eseguono, per le aree di rispettiva competenza, leverifiche e i controlli sui processi in ambito Privacy.
- **Risorse umane:** supporta l'Ufficio Privacy nelle attività relative al rispetto delle disposizioni in tema privacy per il personale dipendente e nel rispetto delle disposizioni stabilite in materia di divieto di controllo a distanza dell'attività dei lavoratori. Supporta inoltre il Gruppo di lavoro nel processo di escalation in caso di violazione delle norme da parte dei dipendenti.
- **Responsabile per la protezione dei dati personali (DPO):** fornisce consulenza al Titolare del trattamento, sorveglia l'osservanza della normativa, fornisce un parere in merito alla valutazione di impatto sulla protezione dei dati e ne sorveglia lo svolgimento, coopera con il Garante e funge da punto di contatto con lo stesso.

5. I PRINCIPI IN TEMA DI PRIVACY

5.1 PRINCIPIO DEL "NEED TO KNOW"

Il need to know è un principio generale che regola il trattamento dei dati personali, appartenenti a categorie particolari e dati relativi a condanne penali e reati, in ogni loro forma di archiviazione, in modo da limitarne l'utilizzo ai soli casi in cui questo risulti necessario e imprescindibile per le finalità per le quali i dati sono stati raccolti. Nello specifico i sistemi informativi e i programmi informatici delle Società del Gruppo bancario ed assicurativo sono configurati in modo tale da ridurre al minimo l'uso di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessatosolo in caso di necessità.

5.2 ACCOUNTABILITY

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del

trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. A fronte di una maggiore discrezionalità lasciata al Titolare del trattamento nel decidere attraverso quali modalità tutelare i dati si introduce l'onere, in capo al medesimo soggetto, di dimostrare le motivazioni che hanno portato all'adozione di una determinata decisione, oltre che di documentare le scelte effettuate.

5.3 PRIVACY BY DESIGN

Il principio della privacy by design prevede che la protezione del dato sia integrata nell'intero ciclo di vita del trattamento, dalla primissima fase di progettazione fino al suo ultimo utilizzo ed all'eliminazione finale.

In particolare, questo principio indica ai soggetti autorizzati al trattamento la necessità di tutelare i dati sin dalla fase di sviluppo, progettazione, selezione nonché utilizzo di applicazioni, servizi e prodotti per il trattamento di dati personali.

Per garantire il rispetto di questo principio il Titolare del trattamento è tenuto ad adottare politiche interne nonché attuare misure tecniche ed organizzative adeguate.

5.4 PRIVACY BY DEFAULT

Il principio della privacy by default afferma la necessità che la protezione dei dati personali debba essere garantita "per impostazione predefinita": il Titolare del trattamento deve garantire che siano trattati di default solo i dati personali necessari per ciascuna finalità specifica del trattamento; e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non debbano andare oltre il minimo necessario rispetto alle finalità perseguite. La minimizzazione costituisce quindi una misura di riduzione del trattamento by default finalizzata ad impostare a priori la massima protezione dei dati attraverso il loro minimo trattamento, sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione dei dati personali, secondo i principi di necessità, pertinenza, adeguatezza e non eccedenza rispetto alle finalità.

5.5 MINIMIZZAZIONE DEI DATI

I dati devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati. Tale tecnica di "sottrazione", portata alle sue estreme conseguenze, conduce all'anonimizzazione dei dati, che si configura come un trattamento che ha lo scopo di impedire l'identificazione dell'interessato. I dati resi anonimi non rientrano nell'ambito di applicazione della legislazione in materia di protezione dei dati. Il principio di minimizzazione dei dati si traduce anche nel principio della limitazione della conservazione.

5.6 TEMPO DI CONSERVAZIONE DEI DATI

I dati vengono trattati per il tempo necessario alla gestione del rapporto con l'interessato, alla cessazione del quale, i dati stessi saranno conservati adottando, dopo tre anni, criteri di minimizzazione del trattamento, fino alla scadenza del termine decennale connesso ad obblighi

di legge e ai termini di prescrizione. Decorso tale ulteriore termine, il Titolare adotta misure tecniche e organizzative per garantire che i dati non siano ulteriormente consultabili, se non per esigenze connesse all'accertamento, all'esercizio o alla difesa di un diritto in sede giudiziaria. Tale ulteriore periodo non eccederà in ogni caso i cinque anni.
In relazione al trattamento per finalità di marketing in caso di manifestazione dei consensi opzionali richiesti, i dati raccolti saranno conservati per il tempo strettamente necessario per la gestione delle finalità sopra indicate secondo criteri improntati al rispetto delle norme vigenti ed alla correttezza ed al bilanciamento fra legittimo interesse di ogni Contitolare e diritti e libertà dell'interessato. Conseguentemente, in assenza di norme specifiche che prevedano tempi di conservazione differenti, i Contitolari avranno cura di utilizzare i dati per le suddette finalità di marketing per tre anni dalla cessazione definitiva di qualsiasi rapporto contrattuale nel rispetto dell'interesse manifestato dalla persona cui si riferiscono i dati verso le iniziative di ogni Contitolare.

6 REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

6.1 REGOLE PER IL TRATTAMENTO PER I DATI ORDINARI (INFORMATIVA E CONSENSO)

Le società italiane del Conglomerato trattano i dati personali in modo lecito e secondo correttezza. La loro raccolta e registrazione avviene per scopi determinati, espliciti e legittimi e i dati personali oggetto di trattamento sono utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi. Tali dati sono esatti, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto le finalità per le quali sono raccolti e trattati. Vengono conservati in una forma tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
La società italiane del Conglomerato informano preventivamente, oralmente o per iscritto, l'interessato o la persona presso la quale sono raccolti i dati personali circa:

- le finalità e le modalità del trattamento;
- la natura obbligatoria o facoltativa del conferimento;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o soggetti autorizzati al trattamento, e l'ambito di diffusione dei medesimi;
- la condivisione di alcuni dati personali fra le Società del Conglomerato in ottemperanza a normative specifiche (ad es. normativa antiriciclaggio);
- i diritti dell'interessato;
- gli estremi identificativi del Titolare e, se designati, del rappresentante nel territorio dello Stato (per il trattamento di quei dati effettuato da chiunque sia stabilito nel territorio di uno Stato extra-UE e impiega strumenti situati nel territorio dello Stato) e del responsabile. Qualora siano stati designati più responsabili è indicato almeno uno di essi, con indicazione del sito della rete di comunicazione o le modalità attraverso cui è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti, è indicato tale responsabile.

Le società appartenenti al Conglomerato trattano i dati personali solo previo consenso espresso dell'interessato. Tale consenso è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato ed è, inoltre, documentato per iscritto a seguito dell'informativa di cui sopra. Il trattamento può essere effettuato in assenza di

consenso per adempiere ad obblighi previsti da leggi, regolamenti, disposizioni emanate da Autorità e Organi di Vigilanza e controllo nonché nei casi espressamente previsti dal Regolamento europeo sulla protezione dei dati.

6.2 REGOLE PER IL TRATTAMENTO DEI DATI APPARTENENTI A CATEGORIE PARTICOLARI

Le società appartenenti al Conglomerato trattano i dati appartenenti a categorie particolari solo previo consenso dell'interessato in forma scritta.

I dati relativi a condanne penali e reati vengono trattati dalle società appartenenti al Gruppo bancario e assicurativo solonei casi di espressa disposizione di legge o di provvedimento del Garante.

6.3 REGOLE PER L'UTILIZZO DI POSTA ELETTRONICA ED INTERNET

Le società appartenenti al Conglomerato specificano le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli. A tal proposito definiscono e pubblicizzano adeguatamente, sottoponendole ad aggiornamento periodico, precise regole sul corretto utilizzo di internet e della posta elettronica, nel rispetto dei principi di necessità e correttezza.
I sistemi software delle società appartenenti al Gruppo bancario ed assicurativo sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica, comprovata e limitata al tempo necessario – e predeterminato – per raggiungere detta finalità.
Le società appartenenti al Conglomerato adottano misure di tipo organizzativo affinché si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza, si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet, si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi.
Le società del Gruppo bancario ed assicurativo adottano, inoltre, misure di tipo tecnologico rispetto alla "navigazione" in Internet per l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa, configurano i sistemi o utilizzano filtri che prevengano determinate operazioni, prevedono il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni, predispongono l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza e la graduazione dei controlli.

Le società del Gruppo bancario ed assicurativo:

- adottano anche misure di tipo tecnologico rispetto all'utilizzo della posta elettronica mettendo a disposizione indirizzi di posta elettronica condivisi tra più lavoratori (eventualmente affiancandoli a quelli individuali);
- eventualmente attribuiscono al lavoratore un diverso indirizzo destinato ad uso privato;
- mettono a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentono di inviare automaticamente, in caso di assenze programmate, messaggi

di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- mettono in grado l'interessato, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa (di tale attività viene redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile);
- inseriscono nei messaggi un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e specificano se le risposte potranno essere conosciute all'interno dell'organizzazione di appartenenza del mittente.

Nell'organizzazione interna per l'utilizzo di posta elettronica e internet e nei relativi controlli le società appartenenti al Gruppo bancario ed assicurativo garantiscono che il trattamento dei dati avvenga nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, tra cui l'art. 4 della Legge 300/1970 sul divieto di controllo a distanza dell'attività dei lavoratori. Le società, per ridurre il rischio di usi impropri della "navigazione" in Internet adottano opportune misure che possono prevenire controlli successivi sul lavoratore.

Relativamente all'impiego della posta elettronica le società del Gruppo bancario ed assicurativo individuano soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

Nell'effettuare gli eventuali controlli, le società rispettano i principi di pertinenza e non eccedenza. Sono preferiti controlli preliminari su dati aggregati o comunque controlli anonimi che si possono concludere con avvisi generalizzati.

6.4 REGOLE PER LA PROFILAZIONE DEI DATI DELLA CLIENTELA

Le società del Gruppo bancario ed assicurativo nel caso in cui svolgano attività di profilazione con dati personali "individuali" operano in ossequio ai principi di necessità e di proporzionalità nel trattamento. L'attività di profilazione è svolta utilizzando solo dati strettamente necessari al perseguimento della finalità e, in ogni caso, trattando solo dati per i quali il Titolare abbia rilasciato una idonea informativa e sia in grado di documentare un consenso libero e specifico dell'interessato.

Tali principi si applicano non solo se la raccolta dei dati è specificamente effettuata per questa finalità, ma anche se l'attività di profilazione viene realizzata mediante dati inizialmente raccolti per una diversa finalità, ivi compresa quella dell'erogazione del servizio.

Le società che intendano procedere al trattamento di dati personali ("individuali" o "aggregati") per finalità di profilazione acquisiscono specifico ed esplicito consenso. Peraltro, il Titolare è in ogni caso tenuto a rendere l'Informativa agli interessati in relazione alle finalità perseguite e ai diritti riconosciuti agli interessati dal GDPR.

6.5 REGOLE IN MATERIA DI AMMINISTRATORI DI SISTEMA

Con il termine "Amministratore di Sistema" si individua generalmente, in ambito informatico,

una figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. La normativa considera tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli Amministratori di Sistema nelle società del Gruppo bancario ed assicurativo sono designati individualmente con elencazione analitica degli ambiti di operatività consentiti, a seguito della valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Gli estremi identificativi delle persone fisiche amministratori di sistema con l'elenco delle relative funzioni attribuite sono riportati in un documento interno che viene mantenuto aggiornato. Tale elenco è disponibile in caso di accertamenti anche da parte del Garante.

Se l'attività degli Amministratori di Sistema riguarda servizi o sistemi che trattano o permettono il trattamento di informazioni di carattere personale di lavoratori, le società rendono nota o conoscibile l'identità di questi nell'ambito delle proprie organizzazioni.

Per quei servizi di amministrazione di sistema affidati in outsourcing il Titolare o il responsabile esterno conservano direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Le società adottano misure organizzative e tecniche idonee alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e vengono conservate per un periodo non inferiore a sei mesi.

6.6 REGOLE IN MATERIA DI VIDEOSORVEGLIANZA

L'installazione di sistemi di rilevazione delle immagini presso le Società del Conglomerato che effettuano trattamenti di dati tramite sistemi di videosorveglianza avviene nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, tra cui l'art. 4 della Legge 300/1970 sul divieto di controllo a distanza dell'attività dei lavoratori.

Il trattamento dei dati tramite sistemi di videosorveglianza avviene nel pieno rispetto del principio di necessità, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali. L'attività di videosorveglianza viene altresì effettuata nel rispetto del principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione delle telecamere nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite. Il rispetto del principio di proporzionalità si applica anche alla durata della conservazione delle immagini, commisurata al tempo necessario e predeterminato a raggiungere la finalità perseguita. Le società rispettano i tempi di

conservazione previsti dalle normative, in ogni caso le immagini non sono mai conservate per un tempo superiore alla settimana e sono cancellate allo scadere del termine previsto.

Gli interessati sono informati, tramite apposita informativa, collocata prima del raggio d'azione della telecamera e chiaramente visibile, che stanno per accedere ad un'area videosorvegliata.

Inoltre, i dati raccolti mediante sistemi di videosorveglianza sono protetti con idonee preventive misure di sicurezza.

Le società adottano specifiche misure tecniche ed organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.

6.7 REGOLE IN MATERIA DI SMALTIMENTO DI RIFIUTI ELETTRICI ED ELETTRONICI

Le società del Conglomerato che, avendone fatto uso nello svolgimento delle proprie attività, non distruggono, ma dismettono supporti che contengono dati personali, adottano idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere reimpiegate o riciclate oppure smaltite.

Nel caso di reimpiego o riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le società adottano misure e accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, nel rispetto delle normative di settore, che consentono l'effettiva cancellazione dei dati o garantiscono la loro non intelligibilità.
Tali misure possono consistere nella:

- cifratura di singoli *file* o gruppi di *file*, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati;
- memorizzazione dei dati sui dischi rigidi dei personal computer o su altro genere di supporto magnetico od ottico in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente.
- cancellazione sicura delle informazioni, ottenibile con programmi informatici che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.
- formattazione "a basso livello" dei dispositivi di tipo hard disk, laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità.
- demagnetizzazione dei dispositivi di memoria basati su supporti magnetici o magnetoottici in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software.

Nel caso di smaltimento di rifiuti di apparecchiature elettriche ed elettroniche le società assicurano l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature attraverso procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi in considerazione del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione;
- demagnetizzazione ad alta intensità.

6.8 REGOLE IN MATERIA DI TRACCIAMENTO DEI DATI

Le società del Gruppo bancario ed assicurativo che trattano dati della clientela, al fine di assicurare il controllo delle attività svolte sui tali dati dei clienti e dei potenziali clienti da ciascun soggetto autorizzato al trattamento, adottano idonee soluzioni informatiche ulteriori rispetto alle misure minime di sicurezza previste dalla normativa nazionale vigente.

Tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dai soggetti autorizzati, sempre che non si tratti di consultazionidi dati in forma aggregata non riconducibili al singolo cliente.

Queste misure sono adottate nel rispetto del divieto del controllo a distanza dell'attività dei lavoratori di cui all'art. 4 della Legge 300/1970 e nel rispetto dei princìpi affermati dal Garante in tema di informativa agli interessati.

I log di tracciamento degli accessi a dati bancari vengono conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione.

Le società hanno prefigurato specifici alert che individuano comportamenti anomali o a rischio relativi agli accessi a dati eseguiti dai soggetti autorizzati al Trattamento.

Il modello organizzativo prevede l'attribuzione della responsabilità delle attività di controllo degli accessi e di anomaly detection, nelle società in cui vi sia trattamento di dati bancari, all'Ufficio Privacy della Divisione Affari Legali di Banca Mediolanum S.p.A. Tale attività di controllo è documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche effettuate su di essi, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. Gli esiti delle attività di controllo sono comunicati alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli, la volontà della Società e vengono messi a disposizione del Garante, nel caso di specifica richiesta.

6.9 REGOLE PER IL TRASFERIMENTO DEI DATI ALL'ESTERO

Se le società appartenenti al Gruppo bancario ed assicurativo trasferiscono, anche temporaneamente, fuori del territorio dello Stato, con qualsiasi forma o mezzo, dati personali oggetto di trattamento, verso un Paese non appartenente all'Unione Europea, le stesse richiedono all'interessato di manifestare il proprio consenso espresso. Nel caso di dati appartenenti a categorie particolari tale consenso è manifestato in forma scritta.

Il trasferimento di dati personali verso un Paese non appartenente all'Unione Europea può altrimenti avvenire quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato.

Il trasferimento di dati personali verso Paesi non appartenenti all'Unione Europea può avvenire anche nel caso in cui risulti necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a

specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato o negli altri casi espressamente consentiti dal GDPR.

Il trasferimento dei dati all'estero è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento UE 2016/679). Al riguardo, possono costituire garanzie adeguate:

senza autorizzazione da parte del Garante:

- gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
- le norme vincolanti d'impresa (art. 46, par. 2, lett. b)
- le clausole tipo (art. 46, par. 2, lett. c e lett. d)
- i codici di condotta (art. 46, par. 2, lett. e)
- i meccanismi di certificazione (art. 46, par. 2, lett. f);

previa autorizzazione del Garante:

- le clausole contrattuali ad hoc (art. 46, par. 3, lett. a)
- gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b)

Tali garanzie sono oggetto di valutazione in sede di verifica precontrattuale ed attestazione di conformità all'interno del Registro dei trattamenti.

6.10 RISPETTO ART.4 DELLO STATUTO DEI LAVORATORI

Le società appartenenti al Gruppo bancario ed assicurativo non utilizzano strumenti per finalità di controllo a distanza dell'attività dei lavoratori.
Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, sono installati soltanto previo espletamento delle formalità necessarie, previste da normative o accordi quadro a livello nazionale. In difetto di accordo la Società provvede a presentare istanza all'ispettorato del lavoro, che detta le modalità per l'uso di tali impianti.

6.11 REGOLE RELATIVE AL CODICE DI CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITÀ E PUNTUALITÀ NEI PAGAMENTI

Il trattamento dei dati personali contenuti in sistemi di informazioni creditizie gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti è effettuato dalle società del Gruppo bancario che partecipano ai suddetti sistemi, in qualità di partecipanti, esclusivamente per finalità correlate alla tutela del credito e al contenimento dei relativi rischi e, in particolare, per valutare la situazione finanziaria e il merito creditizio degli interessati o, comunque, la loro affidabilità e puntualità nei pagamenti. Non viene perseguito alcun altro scopo, specie se relativo a ricerche di mercato e promozione, pubblicità o vendita diretta di prodotti o servizi.
Il trattamento effettuato nell'ambito di tali sistemi riguarda solo dati riferiti al soggetto che chiede

di instaurare o è parte di un rapporto di credito con una società e al soggetto coobbligato, anche in solido, la cui posizione è chiaramente distinta da quella del debitore principale.
Il trattamento non riguarda dati appartenenti a categorie particolari e dati relativi a condanne penali e reati, e concernedati personali di tipo obiettivo, strettamente pertinenti e non eccedenti rispetto alle finalità perseguite, relativi ad una richiesta/rapporto di credito, e concernenti anche ogni vicenda intervenuta a qualsiasi titolo o causa fino alla regolarizzazione degli inadempimenti.
Le società che partecipano ai suddetti sistemi adottano idonee procedure di verifica per garantire la lecita utilizzabilità nel sistema, la correttezza e l'esattezza dei dati comunicati al gestore. Inoltre, verificano con cura i dati da esso trattati e rispondono tempestivamente alle richieste di verifica del gestore.
Dispongono o richiedono al gestore eventuali operazioni di eliminazione, integrazione o modificazione dei dati registrati, da loro comunicati, anche a seguito dell'esercizio di un diritto da parte dell'interessato, oppure in attuazione di un provvedimento dell'autorità giudiziaria o del Garante.
Al verificarsi di ritardi nei pagamenti, la società, anche unitamente all'invio di solleciti o di altre comunicazioni, avvertono l'interessato circa l'imminente registrazione dei dati in uno o più sistemi di informazioni creditizie nel rispetto dei tempi previsti dal Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti Al momento della raccolta dei dati personali relativi a richieste/rapporti di credito, la società appartenente al Gruppo informa, per iscritto secondo il modello predisposto dal Garante, l'interessato anche con riguardo al trattamento dei dati personali effettuato nell'ambito di un sistema di informazioni creditizie. Tale informativa è adeguatamente evidenziata e collocata in modo autonomo ed unitario in parti o riquadri distinti da quelli relativi ad eventuali altre finalitàdel trattamento effettuato.
Quando la richiesta di credito non è accolta, la società comunica all'interessato se, per istruire la richiesta di credito, ha consultato dati personali relativi ad informazioni creditizie di tipo negativo in uno o più sistemi, indicando gli estremi identificativi del sistema da cui sono state rilevate tali informazioni e del relativo gestore e fornisce all'interessato le altre notizie previste dalla normativa nazionale vigente.
Qualora la richiesta di credito non sia accolta o sia oggetto di rinuncia la società ne dà notizia al gestore con l'aggiornamento mensile.
Le società aggiornano senza ritardo i dati relativi alla regolarizzazione di inadempimenti di cui abbiano conoscenza, avvenuti dopo la cessione del credito da parte del partecipante ad un soggetto che non partecipa al sistema, anche a seguito di richiesta dell'interessato munita di dichiarazione del soggetto cessionario del credito o di altra idonea documentazione.
Qualora l'interessato comunichi ad una società del Gruppo partecipante la revoca del consenso al trattamento delle informazioni di tipo positivo, nell'ambito del sistema di informazioni creditizie, questa ne dà notizia al gestore con l'aggiornamento mensile previsto dalla normativa nazionale vigente.
Le società possono accedere al sistema di informazioni creditizie anche mediante consultazione di copia della relativa banca dati, relativamente alle casistiche definite dal Codice di Condotta.
Solo un numero limitato di responsabili e soggetti autorizzati al trattamento dei dati, rispetto all'intera organizzazione, designati per iscritto, accede al sistema di informazioni creditizie, con esclusivo riferimento ai dati strettamente necessari, pertinenti e non eccedenti in rapporto alle finalità indicate, in relazione alle specifiche esigenze derivanti dall'istruttoria di una richiesta di credito o dalla gestione di un rapporto. L'accesso al sistema di informazioni creditizie avviene attraverso le modalità e gli strumenti anche telematici individuati per iscritto con il gestore, nel rispetto della normativa sulla protezione dei dati personali.
Non è in ogni caso possibile effettuare interrogazioni di massa o acquisizioni di elenchi di dati concernenti richieste/rapporti di credito relativi a soggetti diversi da quelli che hanno chiesto di

instaurare o sono parte di un rapporto di credito con la società.
In relazione ai dati personali registrati in un sistema di informazioni creditizie, gli interessati possono esercitare i propri diritti secondo le modalità stabilite dal Codice.
Quando le società trattano i dati contenuti in un sistema di informazioni creditizie mediante l'impiego di tecniche o sistemi automatizzati di credit scoring, assicurano il rispetto dei seguenti principi:

6.11.1 tali trattamenti possono essere effettuati solo per l'istruttoria di una richiesta o per la gestione dei rapporti instaurati;
6.11.2 i dati relativi a esiti, indicatori o punteggi associati ad un interessato sono elaborati e comunicati dal gestore al solo partecipante che ha ricevuto la richiesta dall'interessato o che ha precedentemente comunicato dati riguardanti il relativo rapporto;
6.11.3 i modelli o i fattori di analisi statistica, nonché gli algoritmi di calcolo degli esiti, indicatori o punteggi sono verificati periodicamente con cadenza almeno biennale ed aggiornati in funzione delle risultanze di tali verifiche.

In relazione al rispetto degli obblighi di sicurezza, riservatezza e segretezza le società impartiscono specifiche istruzioni per iscritto ai rispettivi responsabili e soggetti autorizzati al trattamento dei dati e vigilano sulla loro puntuale osservanza, anche attraverso verifiche da parte di idonei organismi di controllo.

6.12 REGOLE IN MATERIA DI CUSTOMER CARE (INBOUND)

Le società del Gruppo bancario ed assicurativo per le attività che comportano un trattamento di dati personali prestate in modalità inbound, ossia oggetto di una chiamata dell'interessato anche se effettuate senza la mediazione di un operatore, utilizzano solo le informazioni personali pertinenti e non eccedenti in relazione ai servizi richiesti. Le informazioni raccolte sono utilizzate per scopi determinati, espliciti e legittimi.

Le società titolari del trattamento attraverso le sopraindicate modalità possono svolgere le attività volte a fornire servizi di assistenza e di informazione al pubblico per via telefonica, tramite personale operante sotto la loro diretta autorità in qualità di soggetti autorizzati al trattamento o terzi cui è affidato il servizio all'esterno sulla base di contratti di collaborazione (c.d. outsourcing). Tali outsourcer vengono designati dal Titolare quali responsabili del trattamento.

Le società effettuano un'analisi preventiva delle implicazioni che il trattamento di dati personali mediante servizi di assistenza telefonica al pubblico potranno comportare, anche tenuto conto della natura dei dati trattati. Il contratto di fornitura del servizio di assistenza telefonica al pubblico contiene le modalità operative idonee ad assicurare condizioni di trasparente e corretto svolgimento delle relazioni con l'utenza e indica altresì le misure di sicurezza idonee che sono adottate, anche al fine di prevenire commistioni tra distinti archivi gestiti dalmedesimo responsabile del trattamento.

Le capacità professionali e l'adeguatezza organizzativa della struttura deputata a svolgere la funzione di servizi di assistenza telefonica al pubblico sono oggetto di particolare cura.

Le registrazioni legittime del contenuto delle comunicazioni sono conservate per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione.

Coerentemente con le disposizioni normative non viene fornita informativa quando non sono

trattati dati personali o in relazione ai diversi elementi già noti all'interessato. Per quei soli casi in cui è invece necessario rappresentare alcuni elementi, vengono utilizzate formule sintetiche, chiare e di immediata comprensione.

6.13 REGOLE IN MATERIA DI COMUNICAZIONE INTEGRATIVA ANNUALE ALL'ARCHIVIO DEI RAPPORTI FINANZIARI

Le società del Gruppo bancario ed assicurativo garantiscono che i soggetti che intervengono nelle procedure di estrazione e di invio per la comunicazione integrativa annuale all'archivio dei rapporti finanziari sono scelti sulla base di elevati requisiti di idoneità soggettiva in termini di affidabilità e competenze.
Sono adottati, per l'invio all'archivio dei rapporti finanziari, meccanismi di cifratura e di sicurezza, rispettivamente finalizzati a proteggere le informazioni contenute nel file durante i successivi passaggi all'interno della società stessa e ad assicurare l'integrità del contenuto e a prevenirne alterazioni. L'accesso al file, nelle fasi del trattamento, è circoscritto ad un numero il più possibile limitato di soggetti autorizzati al trattamento.

Le comunicazioni contenenti dati personali, ancorché cifrati, vengono cancellate da parte dell'operatore dai server di posta utilizzati per la comunicazione, una volta completata la procedura di invio o ricezione.

7. TIPI DI DATI TRATTATI E FINALITA'

7.1. TIPI DI DATI TRATTATI E SOGGETTI CUI I DATI SI RIFERISCONO

I dati trattati dalle società del Gruppo bancario ed assicurativo, classificati sulla base delle linee guida fornite dal Garante, sono riconducibili alle seguenti categorie:

- nominativo, indirizzo ed altri elementi d'identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato e di lavoro, numero di telefono, di telefax, di posta elettronica, posizione rispetto agli obblighi militari, numero carta d'identità, passaporto, patente di guida, n. posizione previdenziale e assistenziale, targa automobilistica, dati fisici quali altezza e peso);
- codice fiscale e altri numeri d'identificazione personale (carte sanitarie);
- dati relativi alla famiglia e a situazioni personali (stato civile, minori a carico, consanguinei, altri appartenenti al nucleo famigliare);
- lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione personale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae o lavorativo, competenze professionali, retribuzione, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente (benefit e altro);
- attività economiche, commerciali, finanziarie e assicurative (dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni, identificativi finanziari, redditi, beni patrimoniali, investimenti, passività, solvibilità, prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi, dati assicurativi, dati previdenziali);
- istruzioni e cultura (curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audio-visivo, ecc. - titoli di studio);

- beni, proprietà, possessi (proprietà, possessi e locazioni, beni e servizi forniti od ottenuti);
- informazioni concernenti i provvedimenti giudiziari di cui all'art. 686, commi 1 (a, d) 2,3 del C.P.P.;
- informazioni concernenti taluni provvedimenti giudiziari;
- dati sul comportamento (creazione di profili umani di utenti, consumatori, contribuenti, profili della personalità e dei tratti caratteriali);
- abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari - ad eccezione di quelle fondate su convinzioni religiose o filosofiche – dati sull'appartenenza ad associazioni diverse da quelle di carattere religioso, filosofico, politico o sindacale sull'orientamento sessuale- licenze, autorizzazioni, licenze di caccia o pesca - dati relativi ad attività sportive o agonistiche);
- stato di salute;
- immagini rilevate attraverso apparecchiatura di videosorveglianza.

Le categorie di soggetti fisici e giuridici interessati a cui si riferiscono i dati, in dettaglio, sono le seguenti:

- personale dipendente;
- lavoratori autonomi;
- candidati da considerare per l'instaurazione di un rapporto di lavoro;
- consulenti e liberi professionisti, anche in forma associata;
- agenti e rappresentanti;
- soci, associati ed iscritti;
- clienti ed utenti;
- potenziali clienti;
- fornitori;
- soggetti od organismi pubblici;
- scolari e studenti di ogni ordine e grado;
- familiari dell'interessato.

7.2. FINALITÀ DEL TRATTAMENTO

Le finalità del trattamento sono riconducibili alle seguenti macro-categorie:

- finalità connesse al settore bancario, di intermediazione e di consulenza in relazione a tutte le attività svolte dalla banca e dalle società del Conglomerato;
- finalità connesse all'attività commerciale;
- finalità amministrative e contabili.

7.3. REGISTRO DEI TRATTAMENTI

È il documento che contiene le informazioni che identificano le finalità del trattamento, le informazioni di dettaglio, le modalità e le misure di conservazione dei dati, le misure di sicurezza applicate e tutti quegli elementi necessari per verificare che gli obblighi normativi previsti dal GDPR siano correttamente rispettati. Dovrà essere tenuto in forma scritta, su supporto tangibile oppure, e preferibilmente, in formato elettronico e dovrà, inoltre, essere messo a disposizione dell'Autorità di controllo. La tenuta del Registro deve consentire una completa ricognizione e valutazione dei trattamenti svolti e deve essere, pertanto, finalizzata all'analisi del rischio.

7.4. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Tale istituto è un processo volto a descrivere un trattamento di dati personali, a valutarne la necessità e la proporzionalità, nonché a gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una ponderazione del livello del rischio e determinando le misure idonee a mitigarlo. Si tratta quindi di un processo che assiste le organizzazioni nell'identificazione e minimizzazione dei rischi derivanti da nuovi progetti e prodotti, secondo modalità riconducibili ad un risk assessment. Qualora il Titolare, a DPIA conclusa, ritenga sia presente un alto rischio residuo per le attività di trattamento dati può chiedere all'autorità Garante di pronunciarsi in merito al trattamento in questione richiedendo una consultazione preventiva.
La valutazione di impatto identifica, classifica e valuta i rischi riscontrati in termini di probabilità e gravità contribuendo a raggiungere un equo bilanciamento tra rischi e benefici. Deve essere sottoposta a revisione periodica almeno triennale o più frequentemente nel caso in cui si registrino variazioni nei fattori di rischio.
Il DPIA va quindi inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali richiesto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (cd. accountability).

8. DIRITTI DELL'INTERESSATO

Le società appartenenti al Conglomerato riconoscono i diritti espressamente previsti dalla normativa a favore degli interessati ed in particolare:

8.1. DIRITTO DI ACCESSO DELL'INTERESSATO

Nel momento in cui viene posto in essere un trattamento di dati personali, l'interessato ha diritto di ottenere dal Titolare l'accesso ai dati che lo riguardano. Per far sì che l'interessato abbia maggiore controllo sulla circolazione dei propri dati, nel caso in cui il trattamento venga svolto con mezzi automatizzati, il Titolare può rendere disponibile la consultazione di detti dati in modo sicuro da remoto. Inoltre, l'interessato ha il diritto di conoscere le finalità perseguite con il trattamento avente ad oggetto i suoi dati, i destinatari a cui verranno comunicati i suoi dati personali, ove possibile, la durata del trattamento ed infine, le eventuali conseguenze di un trattamento basato sulla profilazione.

8.2. DIRITTO ALL'OBLIO

La normativa introduce il diritto dell'interessato ad ottenere la cancellazione dei propri dati personali se non pertinenti o non più pertinenti, o se inadeguati rispetto alle finalità del trattamento, o se l'interessato abbia revocato il proprio consenso, o qualora i dati siano trattati in modo illecito. Pertanto, il Titolare del trattamento è obbligato ad adottare misure adeguate, in base ai mezzi ed alla tecnologia a sua disposizione, per informare altri titolari del trattamento in merito alla richiesta di cancellazione da parte dell'interessato, al fine di eliminare qualsiasi link, copia o riproduzione dei dati personali riconducibili a quest'ultimo.

Infine, bisogna evidenziare che detto diritto all'oblio può essere limitato solo nelle ipotesi elencate dal comma 3 del citato articolo 17 quali ad esempio la garanzia della libertà di espressione, il diritto alla difesa in sede giudiziaria, o per tutelare un interesse pubblico generale.

8.3. DIRITTO ALLA LIMITAZIONE DEL TRATTAMENTO

La normativa definisce espressamente cosa si intenda per "limitazione di trattamento", ovvero il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
Il GDPR elenca, inoltre, le ipotesi in cui l'interessato può esercitare il diritto di limitare l'utilizzo dei suoi dati personali al solo fine della conservazione dei medesimi; in particolare affinché l'interessato possa esercitare tale diritto deve ricorrere almeno una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali;
- i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al Titolare del trattamento non servono più a fini del trattamento;
- l'interessato si è opposto al trattamento e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del Titolare del trattamento prevalgano su quelli dell'interessato.
  Tale limitazione tuttavia dovrebbe risultare in modo chiaro dal sistema al fine di facilitare il relativo esercizio del diritto da parte dell'interessato; questo aspetto deve essere tenuto in considerazione soprattutto nell'ambito della programmazione e dello sviluppo dei sistemi informativi cd. "by design", infatti sarà necessario prevedere una funzionalità di questo genere, per consentire di "contrassegnare" i dati personali memorizzati.

8.4. DIRITTO ALLA PORTABILITA'

La normativa introduce il diritto alla portabilità che consente all'interessato di ricevere i dati personali forniti a un Titolare, in un formato di uso comune e leggibile da dispositivo informatico, e di trasferirli a un altro Titolare del trattamento senza impedimenti.Tale diritto si applica ai trattamenti automatizzati, quindi non trova applicazione in caso di trattamenti effettuati su supporti cartacei; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato medesimo.

8.5. DIRITTO ALL'AGGIORNAMENTO E RETTIFICA

L'interessato può rivolgersi al titolare del trattamento per ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, ha anche il diritto di ottenere l'integrazione dei dati incompleti, eventualmente fornendo una dichiarazione integrativa.
È uno dei diritti che consente all'interessato di mantenere un controllo attivo sui propri dati, potendone ottenere la correzione, la modifica, l'aggiornamento e l'integrazione, così evitando che il loro uso, compreso il trasferimento, possa generare dei pregiudizi per l'interessato.

8.6. DIRITTO DI OPPOSIZIONE

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano connessi a ragioni di interesse pubblico o all'esercizio di pubblici poteri (ai sensi dell'articolo 6, paragrafo 1, lettera e). Si tratta di un diritto che trova la sua ragione di essere nella tutela dell'individuo dal controllo eccessivo dello Stato.
L'interessato può opporsi anche al trattamento posto in essere per il perseguimento di legittimi interessi del titolare o di terzi (art. 6, par. 1, lett. f), compresa la profilazione sulla base di tali disposizioni.
Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
L'interessato può opporsi anche al trattamento dei dati per fini commerciali, come marketing diretto e profilazione

9. SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Il Gruppo Bancario ed il Gruppo Assicurativo prevedono nel proprio modello organizzativo privacy l'esistenza delle figure di seguito riportate con la relativa distribuzione dei ruoli e delle responsabilità.

9.1. IL TITOLARE E IL DELEGATO DEL TITOLARE

Il Titolare è la persona fisica, la persona giuridica e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza. È il reale ed effettivo centro che esercita in completa autonomia il potere decisionale sull'attività di gestione dei dati.

Il Titolare è, per ciascuna Società del Gruppo bancario, la persona giuridica costituita dalla società stessa.

Nel modello organizzativo sul trattamento dei dati di Mediolanum, al fine di una migliore gestione degli adempimenti strettamente connessi alla normativa di riferimento, ogni società nomina un soggetto qualificato cui delegare gli adempimenti propri del Titolare. Il delegato è nominato da e risponde direttamente al Consiglio di Amministrazione per conto del Titolare del trattamento dei dati personali.

Il soggetto delegato, ove necessario, nomina i responsabili esterni per il trattamento dei dati.

9.2. IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Il Responsabile della protezione dei dati è la persona fisica nominata dal Titolare che è

incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

9.3. I RESPONSABILI DEL TRATTAMENTO

I Responsabili sono i fornitori, infra o extra-Gruppo, che, in virtù di un contratto con una Società del Gruppo bancario, effettuano un trattamento di dati di titolarità di quest'ultima, attenendosi alle istruzioni impartite dal Titolare.

Il Responsabile è designato facoltativamente dal Titolare. Se designato, è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza.

Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e delle proprie istruzioni.

Ciascuna Società del Conglomerato conserva ed aggiorna periodicamente l'elenco dei propri Responsabili Esterni del trattamento.

9.4. I SOGGETTI AUTORIZZATI AL TRATTAMENTO E GLI ADDETTI ALLA VIDEOSORVEGLIANZA

Il soggetto autorizzato al trattamento è la persona fisica che materialmente effettua le operazioni di trattamento sotto la diretta autorità del Titolare o del responsabile, attenendosi alle istruzioni impartite.

Il soggetto autorizzato al trattamento viene designato per iscritto previa individuazione puntuale dell'ambito del trattamento consentito.
I soggetti autorizzati al trattamento addetti alla videosorveglianza (autorizzati sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini) sono un numero limitato di soggetti, designati per iscritto dal Titolare o dal responsabile interno designato.

9.5. GLI AMMINISTRATORI DI SISTEMA

Con la definizione di "amministratore di sistema" si individuano figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 Novembre 2008 vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Le Società del Gruppo bancario designano i propri Amministratori di Sistema individualmente, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Ciascuna Società conserva in un documento interno, da mantenere aggiornato e disponibile in caso di ispezione da parte del Garante, gli estremi identificativi degli Amministratori di Sistema designati, con l'elenco delle funzioni ad essi attribuite.

10. LE MISURE DI SICUREZZA

10.1. MISURE ADEGUATE

I dati personali oggetto di trattamento nelle società del Gruppo sono custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

10.2. MISURE MINIME

Nel quadro delle più generali misure idonee di sicurezza adottate dalle Società del Gruppo bancario, le stesse garantiscono l'implementazione delle misure minime di sicurezza, volte ad assicurare un livello minimo di protezione dei dati personali.

Misure minime per i trattamenti effettuati con l'ausilio di strumenti elettronici
Per quanto attiene il trattamento dei dati personali effettuato con strumenti elettronici, le società del Gruppo bancario adottano le seguenti misure minime di sicurezza:

Autenticazione informatica: I soggetti autorizzati al trattamento di dati personali sono

dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un codice univoco per l'identificazione del soggetto autorizzato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo del soggetto autorizzato , eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica del soggetto autorizzato, eventualmente associata a un codice identificativo o a una parola chiave.

Ad ogni soggetto autorizzato al trattamento sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Ai soggetti autorizzati al trattamento è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo e di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili al soggetto autorizzato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati appartenenti a categorie particolari e di dati relativi a condanne penali e reati la parola chiave è modificata almeno ogni tre mesi.

Le credenziali di autenticazione in caso di perdita della qualità che consente al soggetto autorizzato l'accesso ai dati o se non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica anche in caso di perdita della qualità che consente al soggetto autorizzato l'accesso ai dati personali.

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il Titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento del soggetto autorizzato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti autorizzati della loro custodia, i quali devono informare tempestivamente il soggetto autorizzato dell'intervento effettuato.

Sistema di autorizzazione: le società del Gruppo bancario utilizzano un sistema di autorizzazione.

I profili di autorizzazione, per ciascun soggetto autorizzato o per classi omogenee di soggetti autorizzati al trattamento, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza: Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli soggetti autorizzati al trattamento e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista dei soggetti autorizzati al trattamento può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615 quinquies del Codice Penale mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati appartenenti a categorie particolari o relativi a condanne penali e reati l'aggiornamento è almeno semestrale.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Per quelle misure minime di sicurezza di cui le società del Gruppo bancario si avvalgono di soggetti esterni alla propria struttura, ricevono dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico in materia di misure minime di sicurezza.

Misure in caso di trattamento di dati appartenenti a categorie particolari e relativi a condanne penali e reati : I dati appartenenti a categorie particolari o relativi a condanne penali e reati i di titolarità delle società del Gruppo sono protetti contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici.

Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

I supporti rimovibili contenenti dati appartenenti a categorie particolari o relativi a condanne penali e reati, se non utilizzati, sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri soggetti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Misure minime per i trattamenti effettuati senza l'ausilio di strumenti elettronici

Il trattamento dei dati personali effettuato senza l'ausilio di strumenti elettronici nelle società del Gruppo è effettuato nel rispetto delle seguenti misure minime di sicurezza.

Ai soggetti autorizzati al trattamento sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario al trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli soggetti autorizzati al trattamento, la lista dei soggetti autorizzati al trattamento può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Quando gli atti e i documenti contenenti dati personali appartenenti a categorie particolari o relativi a condanne penali e reati sono affidati ai soggetti autorizzati al trattamento dei dati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai soggetti autorizzati al trattamento fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati appartenenti a categorie particolari o dati relativi a condanne penali e reati è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di soggetti autorizzati al trattamento della vigilanza, le

persone che vi accedono sono preventivamente autorizzate.

10.3. DATA BREACH

Per data breach, nella versione italiana violazione dei dati personali, si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Secondo la normativa, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuti a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

11. GLI INTERVENTI FORMATIVI

Per le società del Conglomerato sono previsti interventi formativi al fine di fornire le conoscenze di base in materia di privacy, necessarie al rispetto degli adempimenti e dei controlli previsti nonché di presentare le principali disposizioni normative secondo una chiave di lettura che, oltre ai concetti giuridici, esamini gli aspetti lavorativi, di marketing e comunicazione, dal punto di vista della Società, del cliente e del dipendente.

Tali interventi consistono nel rilascio periodico di corsi online obbligatori per tutti i dipendenti e collaboratori della rete di vendita. Il superamento di tali corsi è subordinato all'effettuazione di un test per verificare l'avvenuta assimilazione dei concetti oggetto dei corsi.

La Società si è posta inoltre l'obiettivo di effettuare specifici programmi di formazione, sensibilizzazione e costante aggiornamento nei confronti della rete di vendita anche attraverso interventi diretti sul territorio.

12. RIFERIMENTI NORMATIVI

I principali riferimenti normativi e regolamentari in tema di rispetto della privacy utilizzati per la stesura del presente documento sono quelli stabiliti in ambito bancario e finanziario, segnatamente:

- Regolamento UE 2016/679 «GDPR»;
- Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti
- Provvedimento del Garante 5 marzo 2007 – «Lavoro: linee Guida in materia di Posta Elettronica e Internet»;
- Esonero dall'obbligo di informativa per i soggetti che fanno parte della catena bancaria (Deliberazione del 26 aprile 2007);
- Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
- Provvedimento del Garante 13 Ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae)e misure di sicurezza dei dati personali;
- Provvedimento 27 novembre 2008 sugli Amministratori di Sistema;

- Provvedimento 25 giugno 2009 in materia di prescrizioni dirette ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione - 6 febbraio 2014. (Aggiornamento);
- Provvedimento 8 aprile 2010 in materia di Videosorveglianza;
- Provvedimento n. 192 del 12 maggio 2011 in materia di Tracciamento delle operazioni bancarie
- Provvedimento n. 229 dell'8 maggio 2014 sulle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookies.
- Disposizioni di attuazione dell'articolo 11, commi 2 e 3, del decreto-legge 6 dicembre 2011 n. 201, convertito, con modificazioni dalla legge 22 dicembre 2011 n. 214, "Modalità per la comunicazione integrativa annuale all'archivio dei rapporti finanziari" – Allegato 4 "Raccomandazioni agli operatori finanziari formulate dal Garante per la protezione dei dati personali"
- Provvedimento del Garante n. 861 del 15 novembre 2012 in materia di "Comunicazione all'anagrafe tributaria da parte di banche e operatori finanziari"